Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	15296	(709/203,217,219,224,227,229).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/02/10 15:03
S1	2	("20030131110").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/02/07 16:47
S2	0	(logon and cook$4 and table).ab.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/02/07 16:49
S3	6	(logon and cook$4).ab.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/02/07 16:54
S4	23	(logon and (cook$4 or credent$5)).ab.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/02/07 16:56
S5	1	(logon and (cook$4 or credent$5) and (multiple of concurrent)).ab.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/02/07 16:55
S6	20	("5757920").URPN.	USPAT	OR	ON	2005/02/09 13:05
S7	18	(authenticat$3 and cook$3).ab.	USPAT	OR	ON	2005/02/09 13:05
S8	18	(authenticat$3 and cook$3).ab. and @ad<= "20020109"	USPAT	OR	ON	2005/02/09 14:36
S9	19	((logon or login or authenticat$3) and cook$3).ab. and @ad<= "20020109"	USPAT	OR	ON	2005/02/09 15:51
S10	2	wo-9946720-$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/02/10 15:02

HPS Trailer Page
for
EAST

UserID: SKlinger_Job_1_of_1

Printer: ran_4c70_gbrfptr

Summary

Document	Pages	Printed	Missed	Copies
US006775670	25	25	0	1
Total (1)	25	25	0	-

US006775670B2

(12) United States Patent
Bessette

(10) Patent No.: **US 6,775,670 B2**

(45) Date of Patent: ***Aug. 10, 2004**

(54) **METHOD AND APPARATUS FOR THE MANAGEMENT OF DATA FILES**

(76) Inventor: **Luc Bessette**, 201-60 de Brésoles,
Montreal, quebec (CA), H2Y 1V5

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/735,585**

(22) Filed: **Dec. 13, 2000**

(65) **Prior Publication Data**

US 2001/0016822 A1 Aug. 23, 2001

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/087,843, filed on May 29, 1998, now Pat. No. 6,263,330.

(51) **Int. Cl.**^{7} **G06F 17/30**

(52) **U.S. Cl.** **707/10**; 707/3; 709/203; 705/2; 705/3

(58) **Field of Search** 707/1, 10, 100, 707/2, 3, 4, 9; 709/203; 705/2, 3, 4

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,715,823 A		2/1998	Wood et al.	600/437
5,845,255 A	*	12/1998	Mayaud	705/3
5,884,246 A		3/1999	Boucher et al.	704/2
5,903,889 A		5/1999	de la Huerga et al.	707/3
5,918,010 A		6/1999	Appleman et al.	709/203

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

WO	WO 98/13783	4/1998
WO	WO 99/44162	9/1999
WO	WO 00/57339	9/2000

OTHER PUBLICATIONS

Li–Hsing Yen, Ting–Lu Huang, and Shu–Yuen Hwang, "A protocol for casually ordered message delivery in mobile computing systems", IEEE, 1997, pp. 365–372.*

C. J. McDonald, J. M. Overhage, W. M. Tierney, P. R. Dexter, D. K. Martin, Jeffrey G. Suico, A. Zafar, G. Schadow, L. Blevins, T. Glazener, J. Meeks–Johnson, L. Lemmon, J. Warvel, B. Porterfield, J. warvel, P. Cassidy, D. Lindbergh, A. Belsito, M. Tucker, B. Williams, C. Wodniak, The Regenstrief Medical Record System: a quarter century experience, International Journal of Medical Informatics 54 (1999), 225–253.

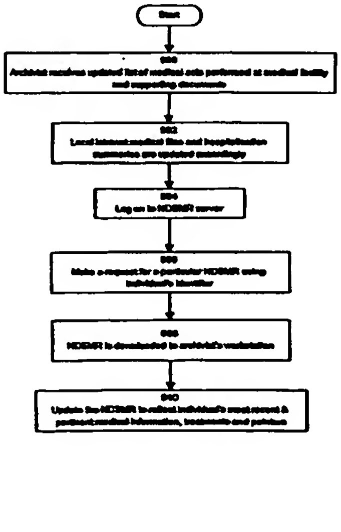
(List continued on next page.)

Primary Examiner—John Breene
Assistant Examiner—Cheryl Lewis
(74) *Attorney, Agent, or Firm*—RatnerPrestia

(57) **ABSTRACT**

The present invention provides a network system for storage of medical records. The records are stored in a database on a server. Each record includes two main parts, namely a collection of data elements containing information of medical nature for the certain individual, and a plurality of pointers providing addresses or remote locations where reside other medical data for that particular individual. Each record also includes a data element indicative of the basic type of medical data found at the location pointed Lo by a particular pointer. This arrangement permits a client workstation to download the record along with the set of pointers which link the client Lo the remotely stored files. The identification of the basic type of information that each pointer points to allows the physician to select the ones of interest and thus avoid downloading massive amounts of data where only part of that data is needed at that time. In addition, this record structure allows statistical queries to be effected without the necessity of accessing the data behind the pointers. For instance, a query can be built based on keys, one of which is the type of data that a pointer points to. The query can thus be performed solely on the basis of the pointers and the remaining information held in the record.

25 Claims, 12 Drawing Sheets


Start
800
Archivist receives updated list of medical acts performed at medical facility and supporting documents
802
Local internet medical files and hospitalization summaries are updated accordingly
804
Log on to HDBMR server
806
Make a request for a particular HDBMR using individual's identifier
808
HDBMR is downloaded to individual's workstation
810
Update the HDBMR to reflect individual's most recent & pertinent medical information, treatments and pointers

U.S. PATENT DOCUMENTS

6,012,083	A		1/2000	Savitzky et al.	709/202
6,018,713	A		1/2000	Coli et al.	705/2
6,263,330	B1	*	7/2001	Bessette	707/4
6,364,834	B1	*	4/2002	Reuss et al.	600/300

OTHER PUBLICATIONS

International Search Report.

Health Networking Solutions, Feb. 1998, http://k12.clearlake.ibm.com/healthcare/solution/hdnsol.html, Global Healthcare Industry. pp. 1–5.

Maintaining a Focus on User Requirements Throughout the Development of Clinical Workstation Software, Janette M. Coble et al., Mar. 1997, pp. 1–10, http://www.acm.org/turing/sigs/sigchi/chi97/proceedings/paper/jmc.htm.

UPMC's Image Engine Project Expands Medical Records System; University of Pittsburgh Medical Center, Mar. 30, 1998, pp. 1–2, http://www.eurekalert.org/releases/uptm–iepjemrs.html.

The Image Engine Project, Prototyping an Internet–Based Multimedia Electronic Medical Record System, Henri J. Lowe M.D., 1997, pp. 1–37, http://www.pathology.pitt.edu/apiii97/talks/lowe/sld001.htm.

Medical Records Projects, Majorie Lazoff M.D., Feb. 1998, pp. 1–6, http://medicalcomputingtoday.com/onvemproj.html.

WWW and the Electronic Medical Record, William M. Detmer, Nov. 29, 1994, pp. 1–11, http://camis.stanford.edu/people/bdetmer/WWWTalk/WWW–outline.html.

World–Wide Web based Electronic Medical Records, Stitt FW, Medix Software Systems, Key Biscayne, Florida USA, University of Miami School of Medicine, Miami, Aug. 1997, pp. 1–7, http://medixb.webnet.net/PAPER/apami.html.

Sharing Electronic Medical Records Across Multiple Heterogeneous and Competing Institutions, Isaac S. Kohane et al., 1996, pp. 1–6.

W3 Based Medical Information Systems vs. Customer Client Server Applications, K.E. Willard et al., 1994, pp. 1–4, http://www.ncsa.uiuc.edu/SDG/IT94/Proceedings/MedTrack/willard/UMHC_www/UMHC_paper.html.

Care web Architecture, pp. 1–2, http://clinquery.bidmc.harvard.edu/people/jhalamka/arch.htm 1999.

TeleMed, Los Alamos National Laboratory, Mar. 1998, pp. 1–32, http://www.acl.lanl.gov/TeleMed/.

An International Collaboratory Based on Virtual Patient Records, David G. Kilman et al., Aug. 1997, pp. 1–7.

The Virtual Patient Record: A Key to Distributed Healthcare and Telemedicine, David Forslund et al., Feb. 29, 1996, pp. 1–4, http://www.acl.lanl.gov/TeleMed/Papers/virtual.html.

Grimson et al., "Interoperability Issues in Sharing Electronic Healthcare Records—The Synapses Approach," 3rd IEEE International Conference on Engineering of Complex Computer Systems, pp. 180– Sep. 8–12, 1997).

Grimson et al., "Federated Healthcare Record Server—The Synapses Paradigm," International Journal of Medical Informatics, vol. 52, No. 1/03, pp. 3–27 (Oct. 1, 1998).

Jagannathan et al., "Corba–Based and Web–Based Patient Records Integration," Proceedings Towards an Electronic Patient Record International Symposium on the Creation of Electronic Health Record System Global Conference on Patient Record, vol. 2, pp. 243–247 (May 13, 1996).

Naszlady et al., "Patient Health Record on a Smart Card," International Journal of Medical Informatics, vol. 48, No. 1–3, pp. 191–194 (Feb. 1, 1998).

Biskup et al., "Cryptographic Protection of Health Information: Cost and Benefit," International Journal of Bio–Medical Computing, vol. 43, No. 1, pp. 61–67 (Oct. 1, 1996).

Morger et al., "Security Concerns for Mobile Information Systems in Health Care," 8th International Workshop on Database and Expert System Applications, pp. 312–317 (Sep. 1–2, 1997).

International Search Report Dated Jul. 14, 1998, pp. 1–3.

* cited by examiner

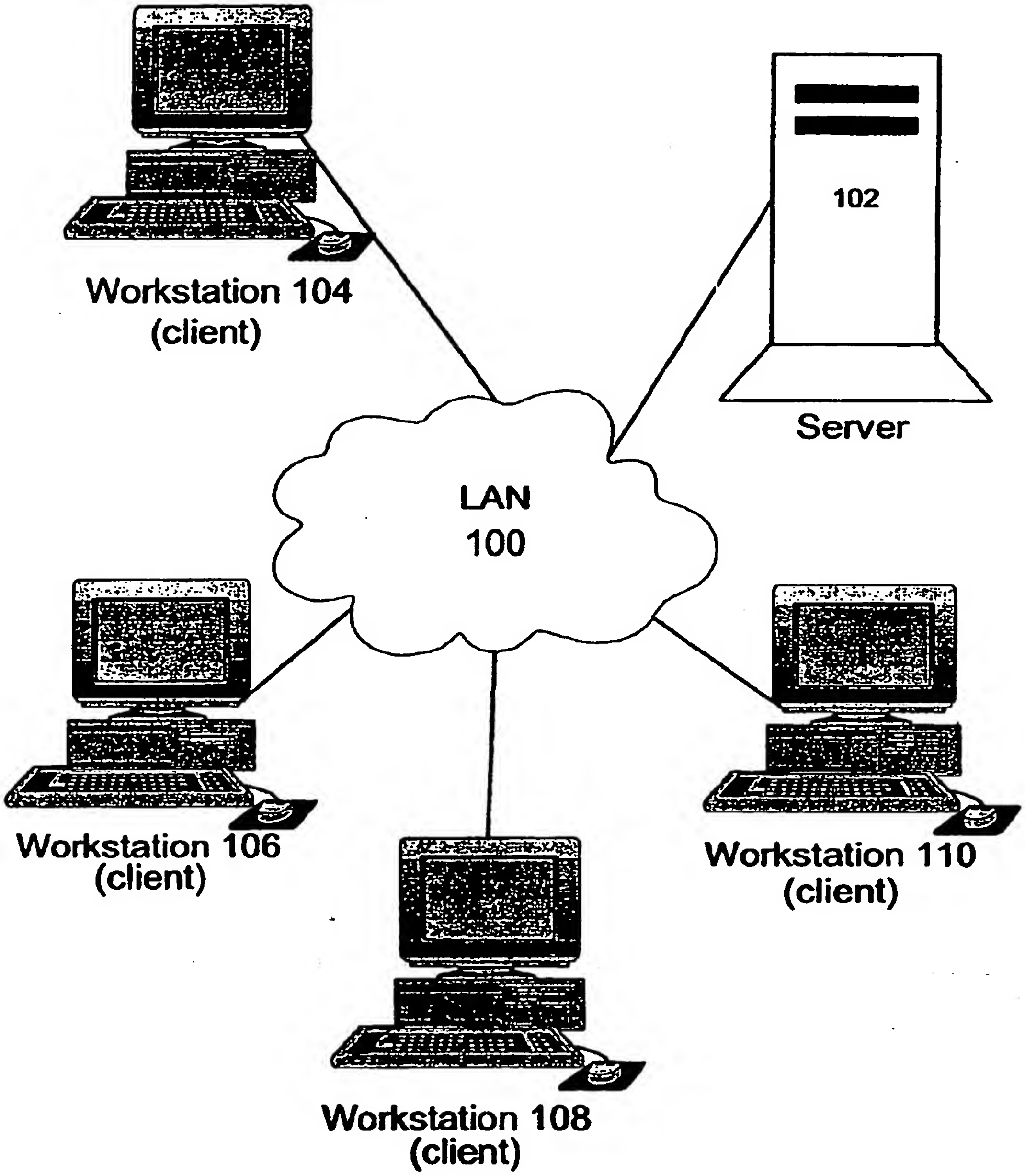

Workstation 104
(client)
102
Server
LAN
100
Workstation 106
(client)
Workstation 110
(client)
Workstation 108
(client)

Figure 1

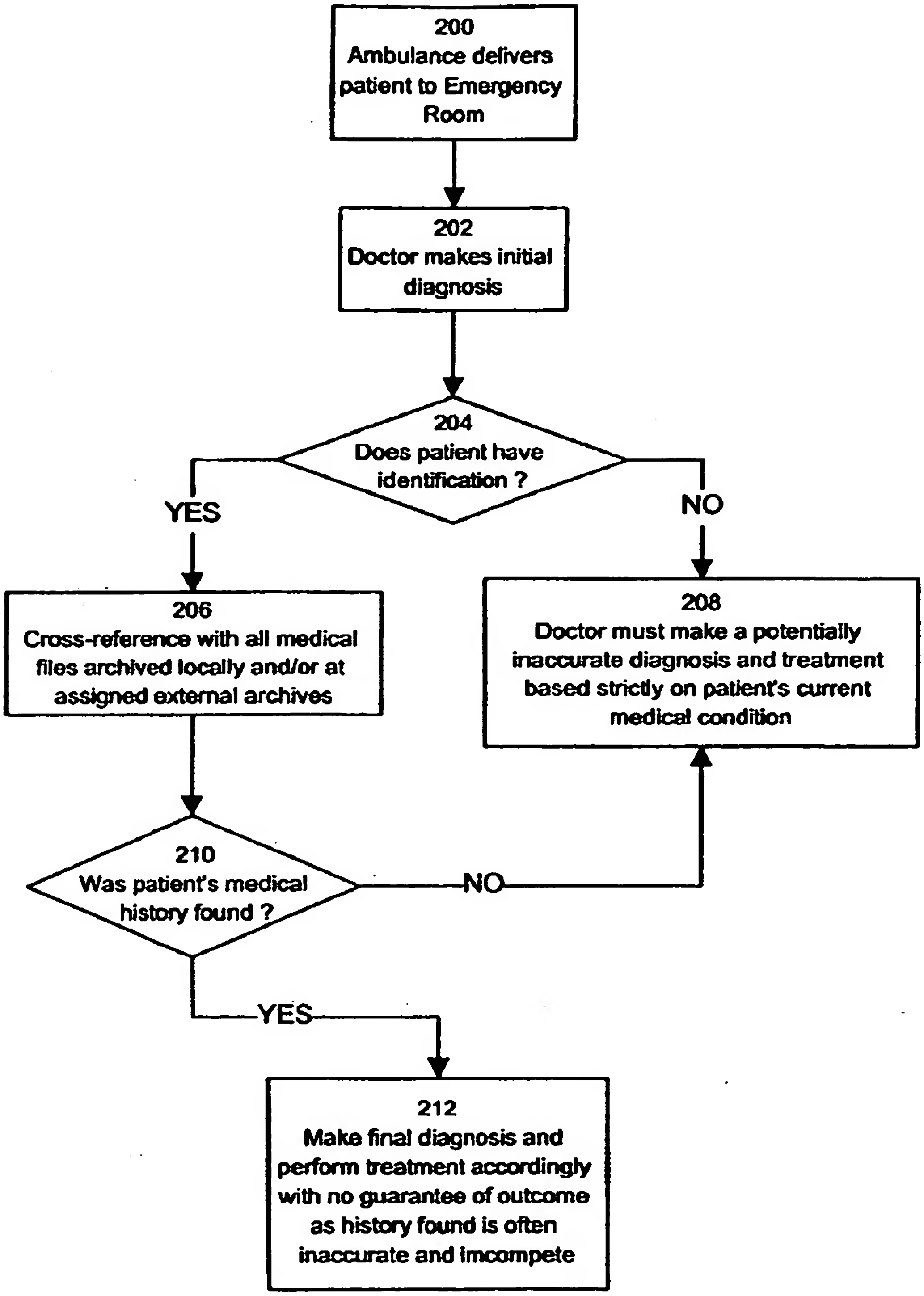

200
Ambulance delivers patient to Emergency Room
202
Doctor makes initial diagnosis
204
Does patient have identification ?
YES
NO
206
Cross-reference with all medical files archived locally and/or at assigned external archives
208
Doctor must make a potentially inaccurate diagnosis and treatment based strictly on patient's current medical condition
210
Was patient's medical history found ?
NO
YES
212
Make final diagnosis and perform treatment accordingly with no guarantee of outcome as history found is often inaccurate and Imcompete

Figure 2

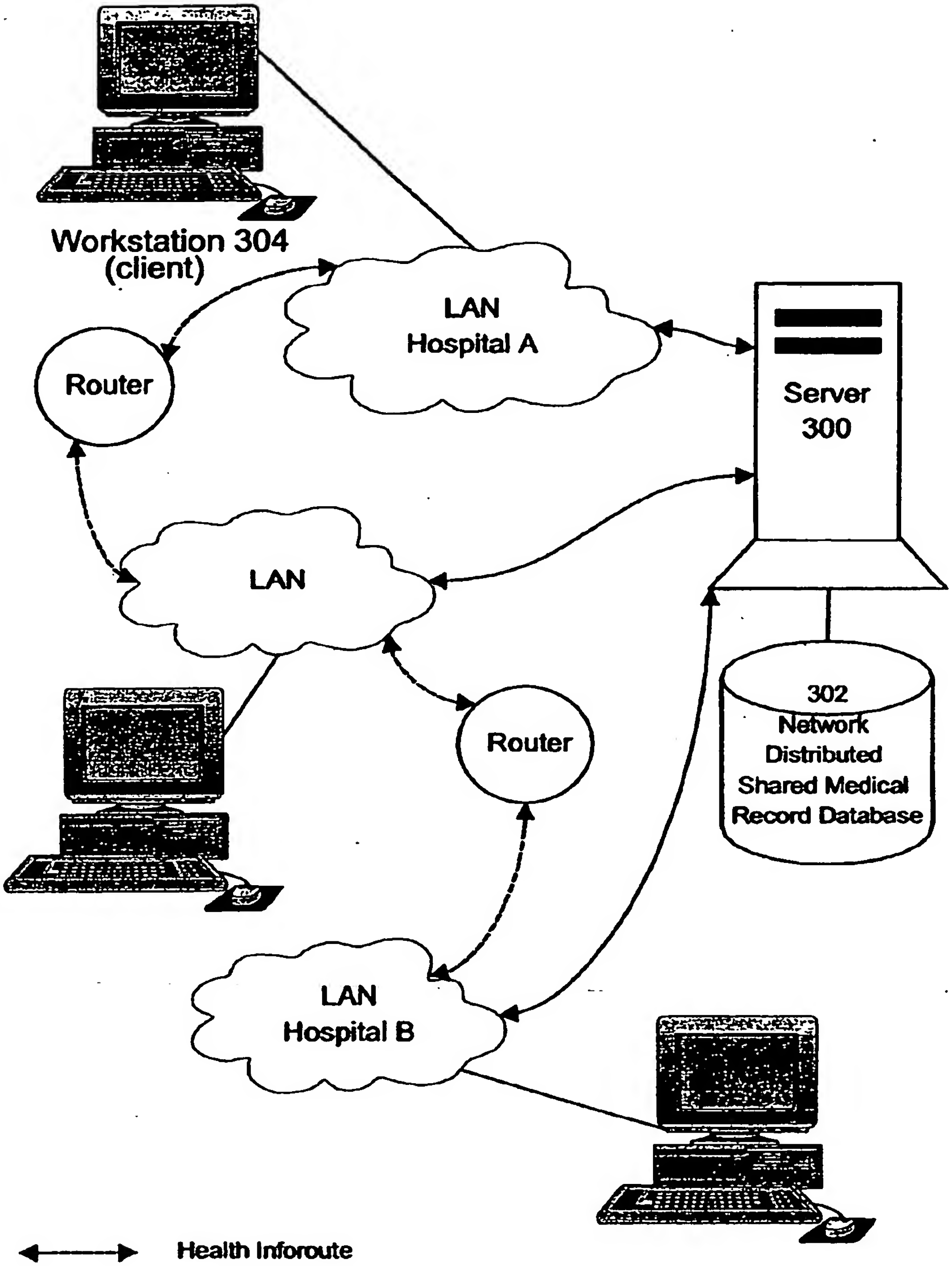

Workstation 304
(client)
LAN
Hospital A
Router
Server
300
LAN
302
Network
Distributed
Shared Medical
Record Database
Router
LAN
Hospital B
Health Inforoute

Figure 3

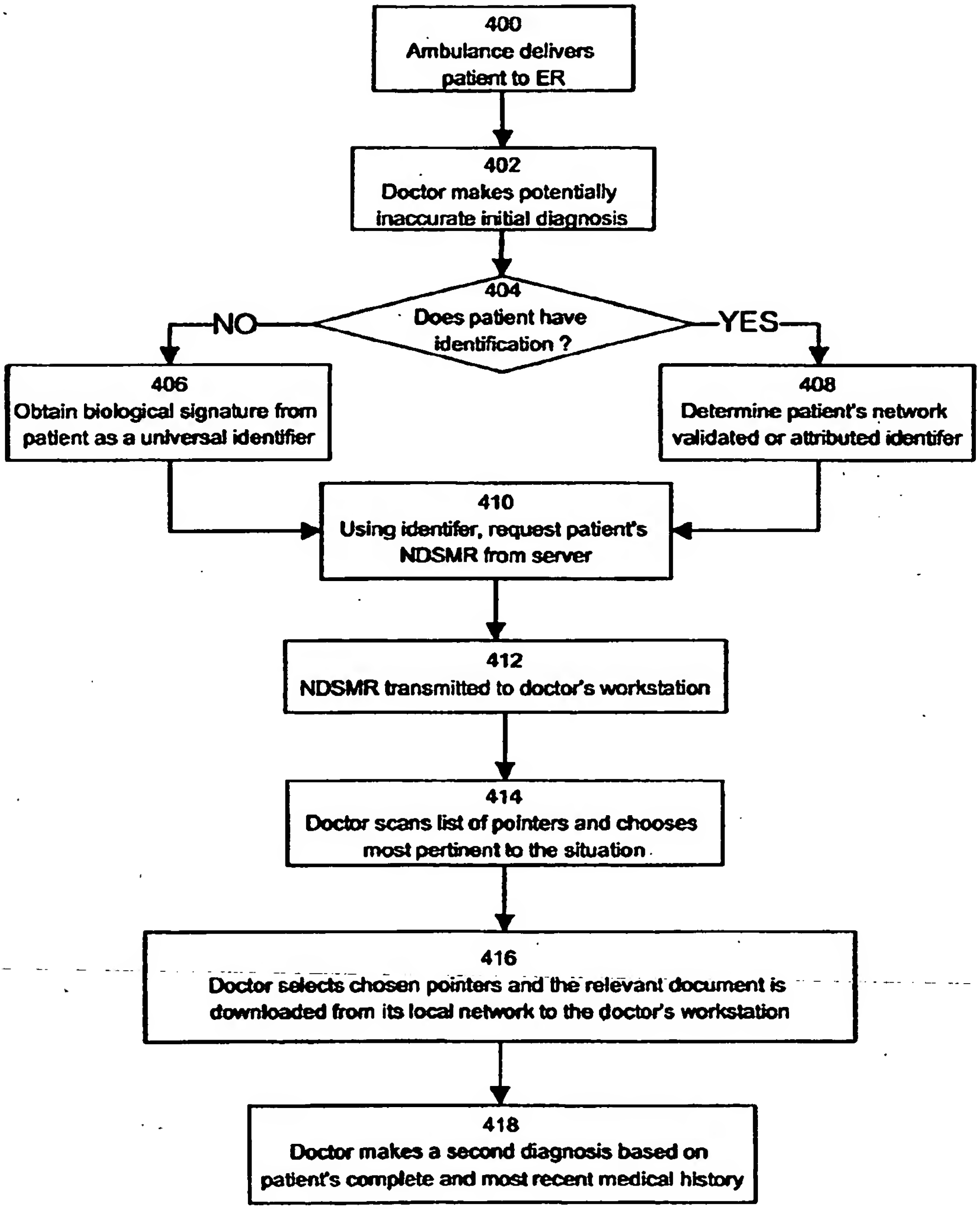

400
Ambulance delivers patient to ER
402
Doctor makes potentially inaccurate initial diagnosis
404
Does patient have identification ?
NO
YES
406
Obtain biological signature from patient as a universal identifier
408
Determine patient's network validated or attributed identifer
410
Using identifer, request patient's NDSMR from server
412
NDSMR transmitted to doctor's workstation
414
Doctor scans list of pointers and chooses most pertinent to the situation
416
Doctor selects chosen pointers and the relevant document is downloaded from its local network to the doctor's workstation
418
Doctor makes a second diagnosis based on patient's complete and most recent medical history

Figure 4

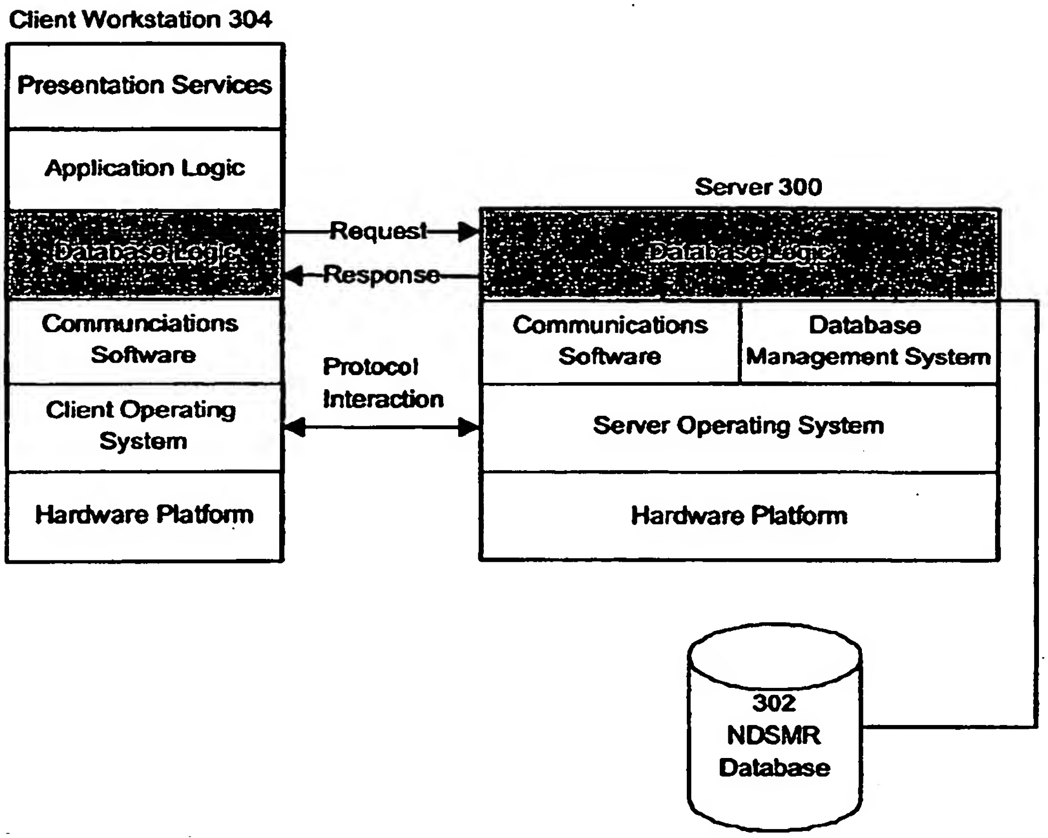
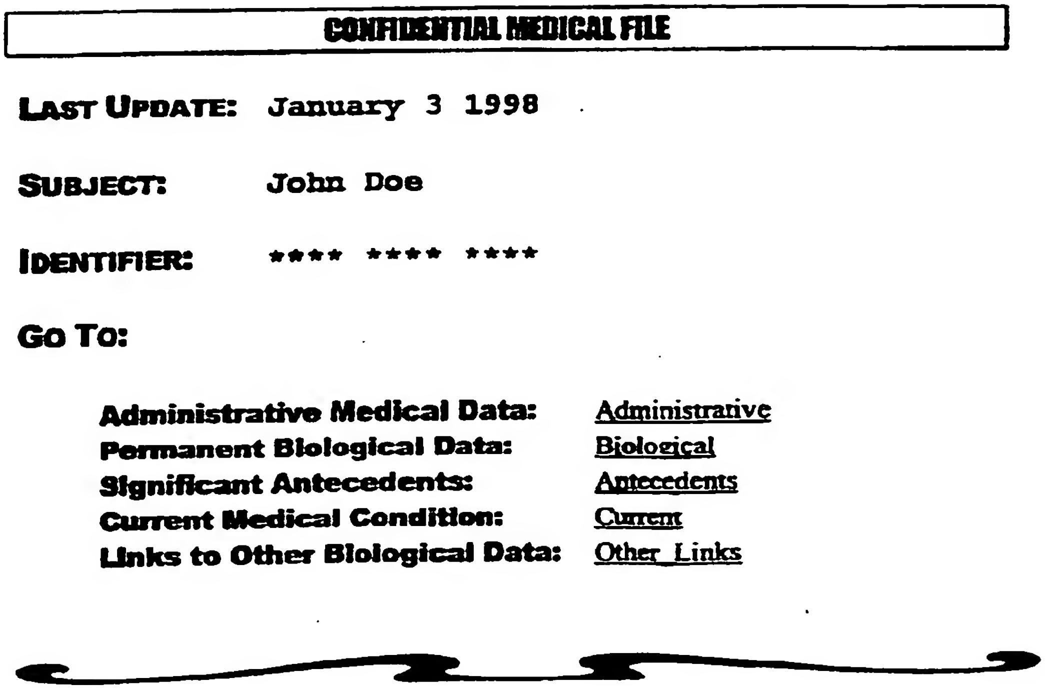

Client Workstation 304
Presentation Services
Application Logic
Database Logic
Communciations Software
Client Operating System
Hardware Platform
Request
Response
Protocol Interaction
Server 300
Database Logic
Communications Software
Database Management System
Server Operating System
Hardware Platform
302 NDSMR Database

Figure 5



CONFIDENTIAL MEDICAL FILE

LAST UPDATE: January 3 1998

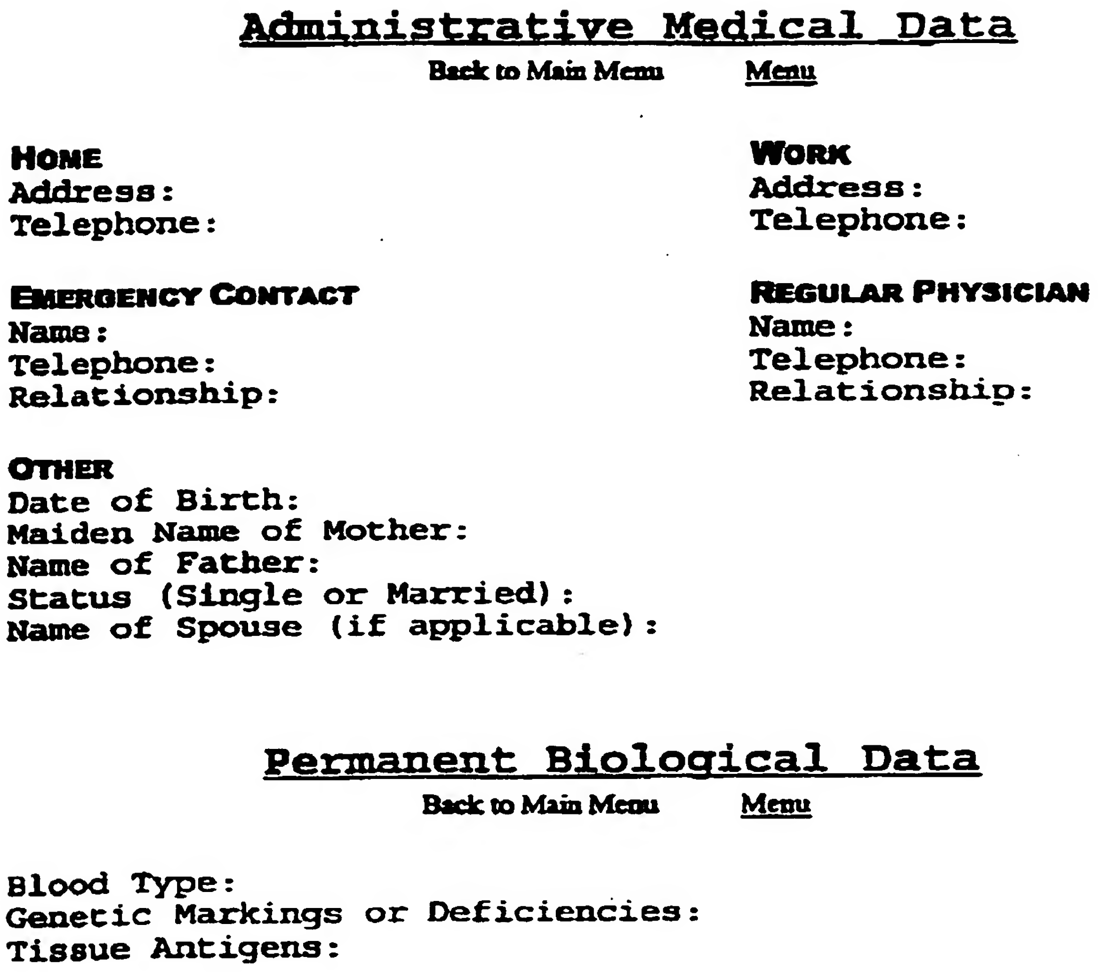
SUBJECT: John Doe

IDENTIFIER: **** **** ****

GO TO:

Administrative Medical Data:	Administrative
Permanent Biological Data:	Biological
Significant Antecedents:	Antecedents
Current Medical Condition:	Current
Links to Other Biological Data:	Other Links

Figure 6A



Administrative Medical Data

Back to Main Menu Menu

HOME
Address:
Telephone:

WORK
Address:
Telephone:

EMERGENCY CONTACT
Name:
Telephone:
Relationship:

REGULAR PHYSICIAN
Name:
Telephone:
Relationship:

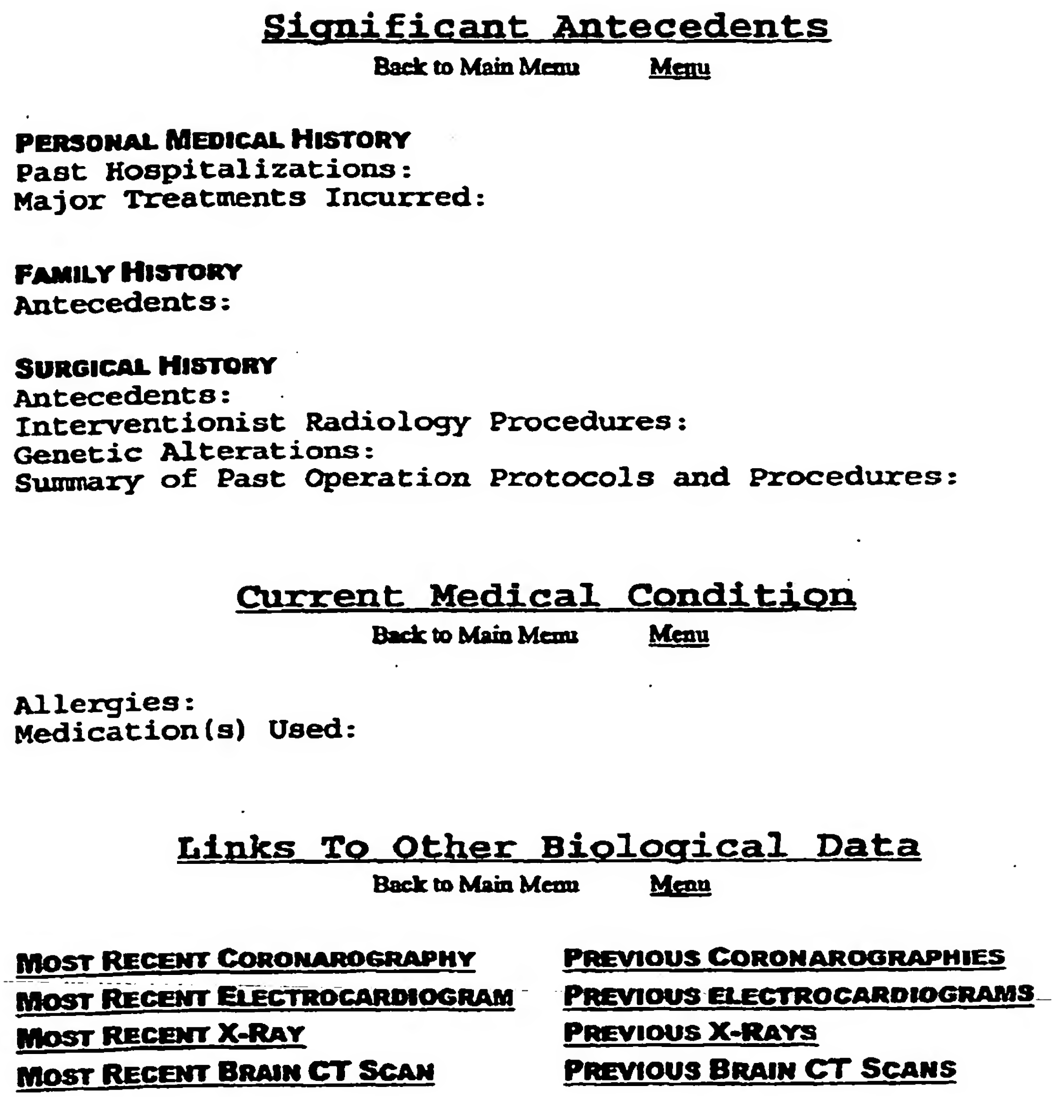
OTHER
Date of Birth:
Maiden Name of Mother:
Name of Father:
Status (Single or Married):
Name of Spouse (if applicable):

Permanent Biological Data

Back to Main Menu Menu

Blood Type:
Genetic Markings or Deficiencies:
Tissue Antigens:

Figure 6B



Significant Antecedents

Back to Main Menu Menu

PERSONAL MEDICAL HISTORY
Past Hospitalizations:
Major Treatments Incurred:

FAMILY HISTORY
Antecedents:

SURGICAL HISTORY
Antecedents:
Interventionist Radiology Procedures:
Genetic Alterations:
Summary of Past Operation Protocols and Procedures:

Current Medical Condition

Back to Main Menu Menu

Allergies:
Medication(s) Used:

Links To Other Biological Data

Back to Main Menu Menu

MOST RECENT CORONAROGRAPHY	PREVIOUS CORONAROGRAPHIES
MOST RECENT ELECTROCARDIOGRAM	PREVIOUS ELECTROCARDIOGRAMS
MOST RECENT X-RAY	PREVIOUS X-RAYS
MOST RECENT BRAIN CT SCAN	PREVIOUS BRAIN CT SCANS

Figure 6C

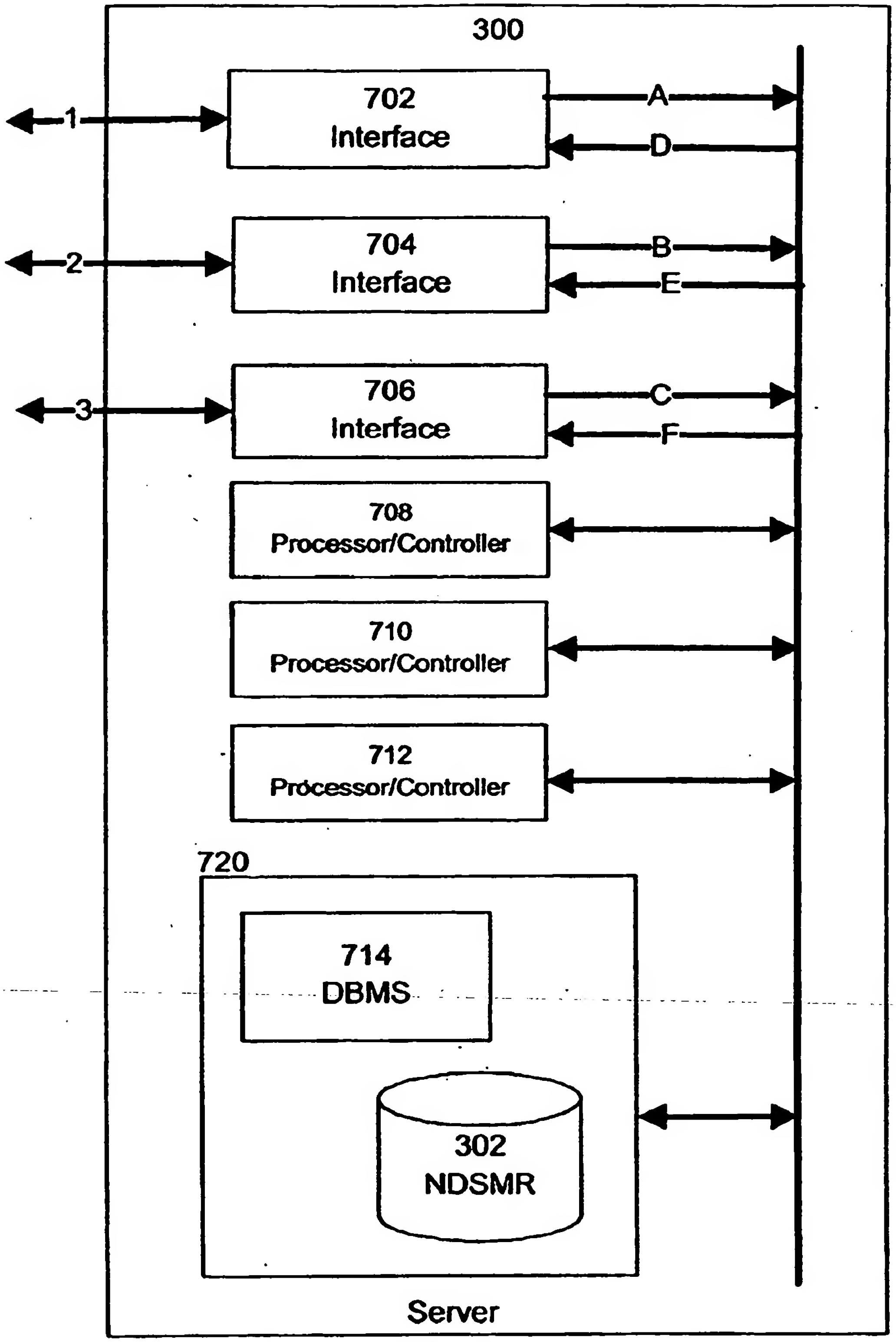

300
1
702
Interface
A
D
2
704
Interface
B
E
3
706
Interface
C
F
708
Processor/Controller
710
Processor/Controller
712
Processor/Controller
720
714
DBMS
302
NDSMR
Server

Figure 7

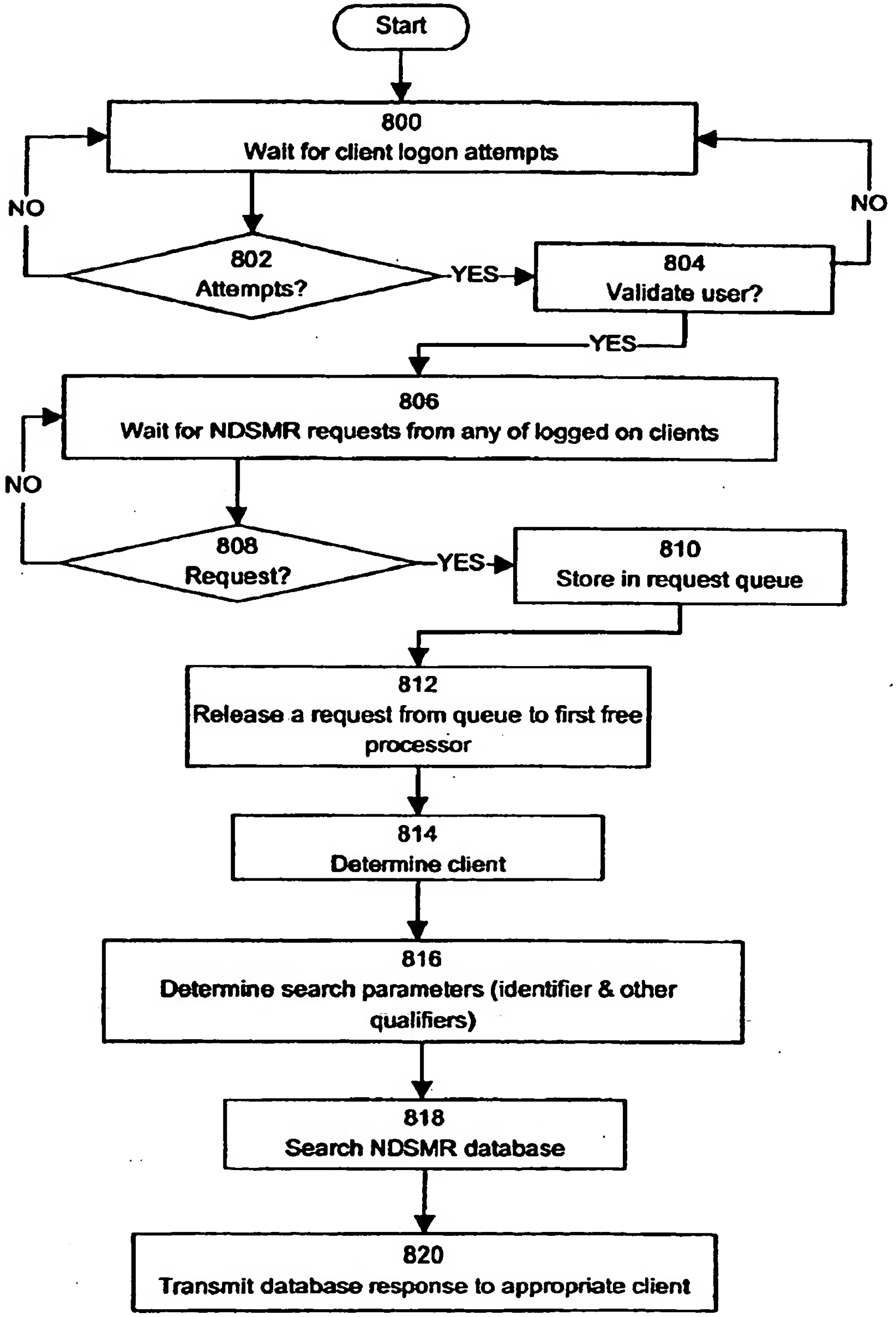

Start
800
Wait for client logon attempts
NO
NO
802
Attempts?
YES
804
Validate user?
YES
806
Wait for NDSMR requests from any of logged on clients
NO
808
Request?
YES
810
Store in request queue
812
Release a request from queue to first free processor
814
Determine client
816
Determine search parameters (identifier & other qualifiers)
818
Search NDSMR database
820
Transmit database response to appropriate client

Figure 8

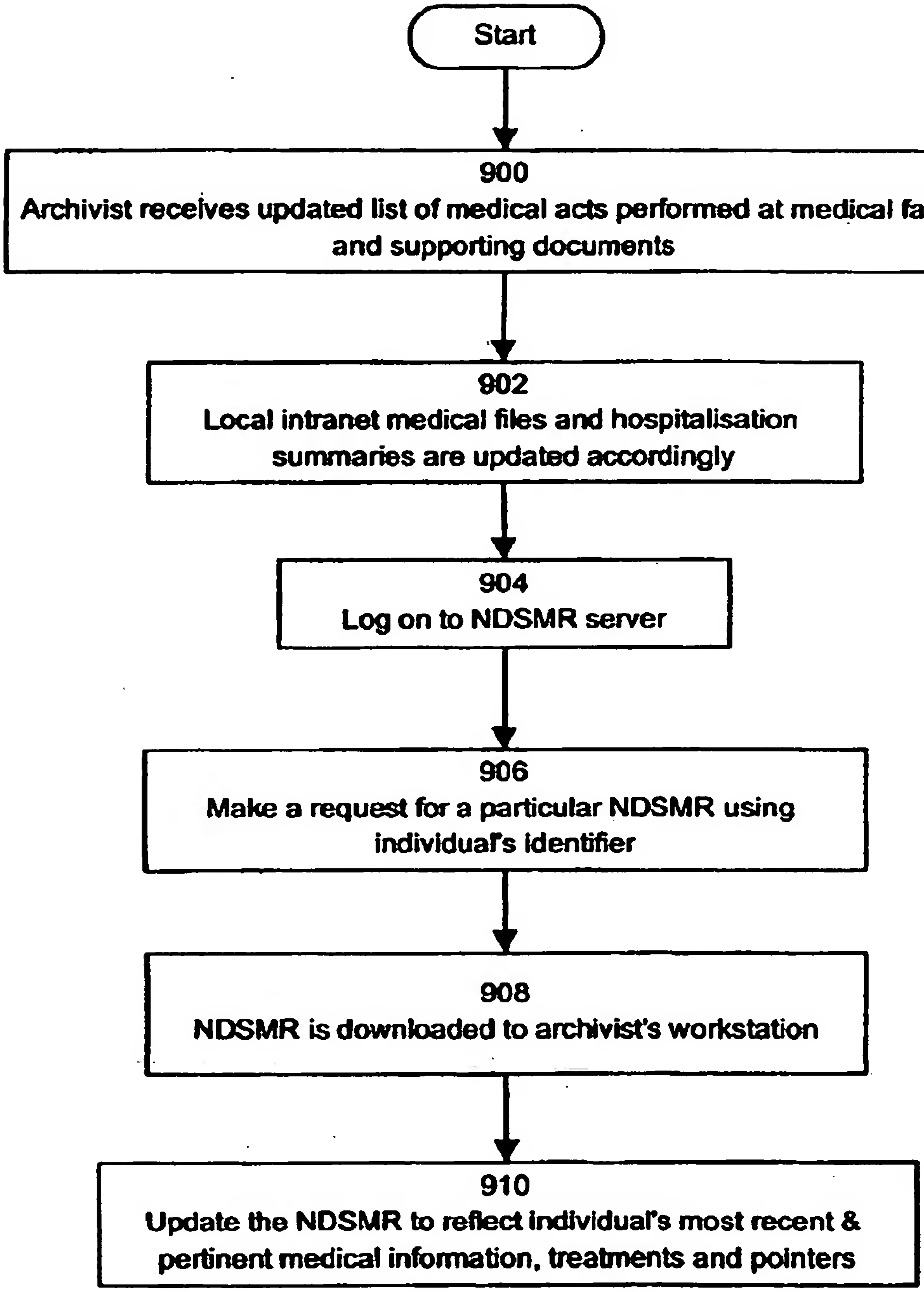

Start
900
Archivist receives updated list of medical acts performed at medical facility and supporting documents
902
Local intranet medical files and hospitalisation summaries are updated accordingly
904
Log on to NDSMR server
906
Make a request for a particular NDSMR using individual's identifier
908
NDSMR is downloaded to archivist's workstation
910
Update the NDSMR to reflect individual's most recent & pertinent medical information, treatments and pointers

Figure 9

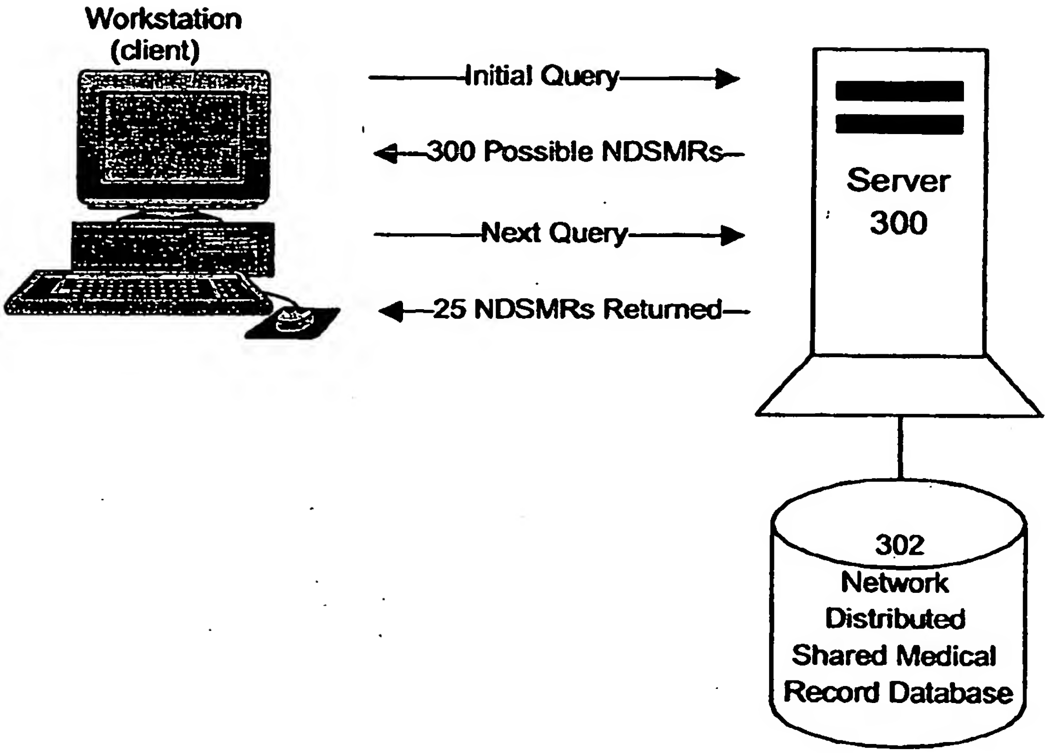

Workstation
(client)
Initial Query
300 Possible NDSMRs
Next Query
25 NDSMRs Returned
Server
300
302
Network
Distributed
Shared Medical
Record Database

Figure 10

METHOD AND APPARATUS FOR THE MANAGEMENT OF DATA FILES

This application is a continuation-in-part of U.S. patent application Ser. No. 09/087,843, filed on May 29, 1998, U.S. Pat. No. 6,263,330.

FIELD OF THE INVENTION

The present invention relates to the field of information distribution systems. More specifically, it pertains to a device and method for the electronic management of data files, for instance within the medical and health education domains.

BACKGROUND OF THE INVENTION

The following paragraphs give definitions of terms relevant to this document:

Client-Server: Client-server computing implies that a single application is being jointly accomplished by two or more interdependent pieces of equipment, including software, hardware and interface. The client requests information and the server provides it, with each one assigned the portion of the job which is suitable to its capabilities. Client-server can be achieved in a local area network of personal computers and servers or by means of a link between a user system and a large host such as a mainframe. Typically, a client-server environment implies a many to one design, whereby multiple clients can make simultaneous requests of the server, allowing for server information sharing between clients. A crucial aspect of Internet Protocol (IP) based technology, such as the World Wide Web (WWW), is the fact that it is a client-server application.

Intranet: An intranet is any internal network (LAN or WAN) that supports Internet applications—primarily web (hypertext transfer protocol), but also other applications such as FTP (file transfer protocol). Intranets are used by many companies to deliver private corporate information to internal users.

Local vs. Wide Area Network: A local area network (LAN) is a private internal communication network that is confined to a small area, such as a single building or a small cluster of buildings. It is a general-purpose local network that can serve a variety of devices, and is generally owned, used, and operated by a single organization. A wide area network (WAN) is similar to a LAN in that it is also a communication network, but a WAN extends over a much broader area, interconnecting communication facilities in different parts of a country. A WAN may also be used as a public utility.

Open System: A system with the capability to cooperate with another system in the exchange of information and in the accomplishment of tasks, where the two systems may be implemented very differently. Every open system must conform to a minimal set of communication and protocol standards, as defined by the open-systems interconnection (OSI) model.

Standard Exchange Protocols: A protocol is the set of rules or conventions governing the way in which two entities cooperate to exchange data. An example of such a protocol is the Internet Protocol (IP), a library of routines called on by various network communications applications.

In the past few years, the worlds of information and technology have made important evolutions. We have progressed from a universal analogical support, usually on paper, towards a theoretically universal electronic support based on the multimedia as well as Internet Protocol (IP) based technology such as the World Wide Web (WWW), JAVA™ and ICQ™ (I Seek You) programs. The transmission of information has also made tremendous progress and is already, or will be soon, practically instantaneous no matter the form of information: text, data, sound, fixed or animated image.

The search for information is becoming more and more similar to the concept of navigation among diverse sources of information and even within documents themselves. The concept of navigation itself implies the need for user accessible tools as well as some sort of structured organization.

Narrowing the focus, this major revolution of information systems brings about profound changes in the relations between academic and hospital domains, in particular everything which deals with medical archives and databases as well as the ability to consult aggregates of these in a transparent way and to share in real or delayed time the information obtained. The number of information sources is multiplying and the communication networks are proliferating: more and more documentation is available in digital form and the information highway is rapidly expanding. Concerning medical archives and databases, questions arise as to their role of maintaining or distributing information. If their roles of acquiring, cataloging and maintaining information are to continue, they will have to give access to the available information on new multimedia supports as well as serve as access points to the information within enlarged networks (e.g. the Healthcare Inforoute™ network). These changes will add to the complexity of their management, all the while enlarging their traditional mandate.

In other words, the medical archives and databases of the future will not only be locally archived medical-legal clinical documents, but also high-performance data banks of primary importance to the practice of medicine and health care everywhere within our network, all the while constituting a living core dedicated to clinical and scientific research and development.

The above described evolution of the medical file and database system requires that the following two objectives be achieved:

- effective navigation across multiple and diverse sources of information, both local and distant, performed in a transparent way with respect to the end user;
- efficient file management allowing universal research, the treatment of contained information, and the sharing of information between system users.

Currently, in order to store medical archives and databases, passive data accumulation for each medical facility takes place within a local network. Unfortunately, the costs of stocking information and storing files in a local network are quite high and the space available is limited. There is also a well-established historical insufficiency concerning the ability of the local medical archive file networks to respond to the documentary and informational needs of the emergency doctor or of the consultant. The medical facilities do not have access to a complete ensemble of information sources, thus complicating emergency medical procedures and diagnoses all the while hampering the facility's ability to give patients the most appropriate treatment.

Although the solution of combining the multiple independent local networks into a single integrated health network seems rather obvious, the implementation of such a concept presents certain problems concerning the manner in which medical data is currently recorded and treated, at both text and image levels. First of all, each separate medical facility may count up to hundreds of thousands of active files, some archived locally, others externally, either in an integrated or a refined form. Second of all the file organization may be different at each facility, a huge obstacle to the merging of all files into a system which supports a common format file organization. There is also the problem of available space when considering the large volume of information contained in each file and the fact that the life of a particular medical file may approach up to twenty-five years in length. Thus volume and merging problems lead to the conclusion that it is currently almost impossible to combine and digitize the whole of all local medical records from all local networks.

Even if the merging and digitizing were possible, there is a question as to whether this would be desired. The data recorded in the medical files does not all have the same informational and discriminatory value in the long run. In fact, the data falls into three categories: data with strict medical-legal value, data with short term clinical value and data with historical value or a biological signature. Unfortunately, the first category, data with strict medical-legal value, makes up the majority of data recorded in the file while it represents the least valuable information for emergency doctors and consultants. On the other hand, the most valuable information for emergency procedures and diagnoses, the third category, makes up a very small portion of data recorded in the file. Therefore an integrated file management system which combines all of the information currently held in archived medical files would be extremely inefficient in terms of usage of space, thus impairing the extraction of information pertinent to a particular research.

The background information herein clearly shows that there exists a need in the industry to provide a method for developing the information highway to allow for access to shared medical files in an enlarged health network and other external databases in order to increase the number of available sources of information for doctors and consultants.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a system and method for electronic management of data files.

Another object of the invention is a computer readable storage medium containing a data structure that holds information.

As embodied and broadly described herein, the invention provides a computer readable storage medium holding a data structure, said data structure comprising at least one record associated with a certain individual, said record including:

at least one unique identifier associated strictly with the certain individual;

at least one pointer, said pointer using the URL addressing system to indicate the address of a location containing data for the certain individual, said address being in a form such that a machine can access the location and import the data from the location;

at least one data field, said data field associated with said pointer, said data field being indicative of the basic nature of the data at the location pointed to by the said pointer.

In a preferred embodiment, the computer readable storage medium is a database containing a large number of medical records for respective individuals. The information in each record includes at least one attributed identifier distinguishing one record from another one. The record also contains one or more pointers, where these pointers use the URL addressing system in order to point to remote sites holding files that contain information in digitized form pertinent to the individual. That information may be blood tests, electrocardiograms among many other possibilities. Each pointer provides an address that is machine readable to import the data residing at the target location. Associated directly with the pointer is a data field, possibly stored in a mapping table in the memory of the Network Distributed Shared Medical Record (NDSMR) server, where this data field contains data indicative of the basic nature of the information held in the file or resource to which the pointer is directed. For the purposes of this specification, the term "associated" implies that the data field is either in a direct one-to-one mapping relationship with the pointer or, alternatively, is integrated with the pointer address to form the actual pointer data structure. Each record may also contain a collection of data elements that provide medical information that is intended to be stored in the record for easy retrieval. This information is typically data that is not likely to change during the lifetime of the individual. In a specific example, the data can include, among others, biological data pertinent to the individual, for instance blood type.

In use, the database can be remotely queried to extract the record associated with a certain individual. Typically, this operation can be performed over a network, where a client workstation requests the record from a server managing the database. The server will transfer over the network links the record that will be displayed on the client workstation. The information displayed includes the collection of data elements permitting to identify the person, as well as any medical data stored in the record, where this data is more or less of a static nature. The operator at the workstation, typically a physician, will also observe one or more pointers to files holding additional medical data. The second part of each pointer, the data part, indicates to the physician the basic nature of the data pointed to. He can therefore select the pointers of interest in the global set of pointers for that record and import the data through any appropriate data transfer protocol.

This arrangement allows the establishment of an electronic medical file system of distributed nature where the bulk of the data is held at sites remote from the central database. Those remote sites are typically the locations where the data would be collected, such as hospitals. Accordingly, the system is very flexible as the records can be maintained even when a patient seeks medical attention and treatment at different sites. Take the example of a patient that visits Hospital A where an electrocardiogram is taken. The electrocardiogram is digitized, by simple optical scanning, and a file created in a local network of Hospital A. An archivist then accesses the remote database and adds a new pointer entry to the patient's record. If, at a later date, the patient visits another hospital, say Hospital B, for the same procedure, another file is created and the appropriate entry made in the patient's database record. Thus, the bulk of the medical data is retained in various locations, yet it can be easily accessed through the pointers' structure.

Although the invention is better suited for applications where the medical records of patients are held in a database, the same inventive principles can also be used for applications where a single record is stored in the machine readable storage medium. Such a storage medium could be a portable memory device, of the so called."Smart Card" type. The portable memory device includes a single record, however, the data structure is the same, namely a collection of data elements of static, medical nature and at least one pointer toward a location containing additional medical information. To use such a portable memory device, it suffices to provide a suitable reader to extract the information contained therein and then to process the information accordingly, such as by remotely accessing and importing the data pointed to by the pointer(s).

In a specific, non-limiting example of implementation, a personal communication system (PCS), such as a cellular phone, can be used to access the NDSMR database. The PCS is equipped with the same communication exchange protocol as that in use by the NDSMR server **300**, such that a connection may be established between the PCS and the NDSMR server **300**.

Accordingly, users of the NDSMR system, including patients that are registered with the NDSMR system as well as healthcare professionals, can benefit from convenient, mobile means for accessing and using the NDSMR system. Other examples of such a PCS include a web phone, a cellular notepad, an IP television screen or monitor, among others.

As embodied and broadly described herein, the invention also provides a network server, including:

a processor;

a memory including:

a) a plurality of records associated with respective individuals, said record including:

i) at least one unique identifier associated strictly with the respective individual;

ii) at least one pointer, said pointer using the URL addressing system to indicate the address of a location containing data for the certain individual, said address being in a form such that a machine can access the location and import the data from the location;

iii) at least one data field, said data field associated with said pointer, said data field being indicative of the basic nature of the data at the location pointed to by the said pointer.

b) a program element including individual instructions, said program element implementing a functional block comprising means responsive to a request to transfer a particular record of said plurality of records towards a client connected to said server through a data communication pathway for locating the particular record and transferring the record toward the client over the data communication pathway.

As embodied and broadly described herein, the invention also provides a network system for distributed storage of records, said network system including:

a server managing a database, said database containing a plurality of records of respective individuals, each record including:

a) at least one unique identifier associated strictly with the respective individual;

b) at least one pointer, said pointer using the URL addressing system to indicate the address of a location containing data for the certain individual, said address being in a form such that a machine can access the location and import the data from the location;

c) at least one data field, said data field associated with said pointer, said data field being indicative of the basic nature of the data at the location pointed to by the said pointer.

a plurality of nodes remote from said server, said nodes being connected to said server through data communication pathways, said nodes constituting locations pointed to by pointers in records of said database and including machine readable storage media holding the data pointed to by pointers in record of said database.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a generic client-server environment, where clients and server are linked by a local area network (LAN);

FIG. **2** is a flowchart which describes the current diagnostic process that takes place in medical facilities;

FIG. **3** is a block diagram of the health inforoute integrated with the Network Distributed Shared Medical Record (NDSMR) System, in accordance with the invention;

FIG. **4** is a flowchart which describes the diagnostic process which will take place in medical facilities under the NDSMR System;

FIG. **5** is a block diagram of a general client-server architecture;

FIGS. **6A**, **6B** and **6C** represent the NDSMR document layout in accordance with a particular embodiment of this invention;

FIG. **7** is a block diagram of a server in accordance with this invention;

FIG. **8** is a flowchart of the program element in accordance with this invention;

FIG. **9** is a flowchart of the update process performed by the archivists on the NDSMRs, in accordance with this invention;

FIG. **10** is a block diagram of the search engine (query) process implemented by the NDSMR system.

DETAILED DESCRIPTION

FIG. **1** illustrates a generic client-server environment, enabled by a local area network (LAN). Client-server computing is a cooperative relationship between one or more clients and one or more servers. The clients **104**, **106**, **108** and **110** submit requests to the server **102**, which processes the requests and returns the results to the clients. Although the processing is initiated by the client(s), both client(s) and server cooperate to successfully execute an application. Therefore, the interaction between the client and the server processes is a transactional exchange in which the client is proactive and the server is reactive. In addition to clients and server, the third essential component of the client-server environment is the network. Client-server computing is distributed computing. In other words, users, applications, and resources are distributed in response to business requirements and are linked by a single LAN **100** or by an Internet of networks.

Currently, most medical facility archives still operate on a paper based support system. However, the higher end medical facilities are set up with their own LAN for archiving medical files, and the computing system is often modeled after the client-server system shown in FIG. **1**. Since each separate facility has its own LAN for archiving files, the accessibility to files of a particular LAN is limited to the workstations linked to that particular LAN. FIG. **2** depicts an example of the current state of affaires faced by medical facilities. Assume an ambulance delivers an unconscious patient to the ER at step **200**. At step **202**, the doctor makes an initial diagnosis, but needs access to the patient's medical history in order to prevent any misdiagnosis. If the patient is without identification of any kind, the doctor has no other recourse but to administer a treatment at step **208** based on a diagnosis that is potentially inaccurate because it has been established strictly on the patient's current medical condition, without taking into account his/her previous medical history. If the patient does have an identification of some kind, it can be used to cross-reference all of the hospital's medical files, archived locally and/or at assigned external archives, at step 206. The patient's file will only be found if the patient was previously treated at the same hospital and already has a file stored in the network server's database. If the file is not found, the doctor is back to step 208. Even if the file is found, it is often incomplete and inaccurate as it lacks the information concerning treatment (s) administered in other medical facilities. Therefore, at step 212 the doctor must make a final diagnosis and perform the corresponding treatment.

FIG. 3 depicts an integrated health network embodying the principles of this invention. For the purposes of this specification, the word "integrated" implies the implementation of internetwork communication between all of the various medical facility LANs, as well as with external sources such as the global Internet, the pharmaceutical network, on-line medical libraries and journals, among many other possibilities. An important component of this network is a Network Distributed Shared Medical Record (NDSMR) system that includes two main components, a server 300 and a NDSMR database 302, with the potential for each LAN within the health network to be connected to the server 300. Alternatively, the system may include more than one server, all operating inter-cooperatively in order to manage the NDSMR database, a resource shared by all of the servers. Although such integrated medical networks may be restricted to a particular geographical region, due to differing medical jurisdictions within a country or between different countries, it is an integration hurdle which could eventually be overcome as a result of a concept of the current invention known as an individual's biological signature, to be described in detail below. The integration of medical facilities could thus someday be national wide, or even international wide, thereby enlarging and improving the health network.

FIG. 4 is a flowchart depicting the improved diagnosis process as a result of the present invention. Assume that an ambulance delivers an unconscious patient to Hospital A. Also assume that the patient is a network user of the health network, and therefore has a personal file stored in the NDSMR database. After the doctor makes his initial diagnosis at step 402, the patient is checked for identification.

If the patient does have identification, his/her network validated or attributed identifier will be known at step 408. In the most preferred embodiment of this invention, such an identifier consists of the patient's medical insurance number such as the one available in a number of countries of the world, including Canada. Alternatively, the identifier may consist of the patient's social insurance number, Smart Card, or any other network attributed identification. A Smart Card is an integrated circuit based card containing individual specific medical information, to be read from and written to by appropriate electronic means, and offers several implementation alternatives to the NDSMR system, to be described in more detail below. If the patient does not have identification, his/her biological signature can be obtained as a universal identifier at step 406. In the most preferred embodiment of this invention, such an identifier consists of a fingerprint derived signature. The technology needed for the implementation of system user identification via a fingerprint derived biological signature could be software similar to that created by and available from delSecur, a Montreal based company. Alternatively, the identifier may consist of a patient's retinal or genetic derived signature, or any other type of biological signature.

At step 410 the doctor sits down at workstation 304 and logs onto the server 300, as will be discussed below. When prompted, the doctor uses the identifier obtained at either step 406 or step 408 in order to request the patient's NDSMR from the server 300. The record is transmitted from the NDSMR database 302 to the doctor's workstation. Once the doctor has read the pertinent medical information found in the record, he/she can scan a list of pointers appended to the record. As will be further described below, these pointers represent various significant medical documents (such as x-rays, surgical reports, etc.), and by their textual or visual representation allow the doctor to determine which of the pointers refer to documents pertinent to the patient's current medical condition. Specific to this example, the doctor decides at step 414 that a pointer referring to the most recent electrocardiogram taken at Hospital B would be helpful for diagnosis, and at step 416 he/she activates the corresponding pointer. Consequently, the document is downloaded over the health network from Hospital B's LAN to the doctor's workstation.

FIG. 5 is a general representation of the client-server architecture that implements the NDSMR system. The system includes three main components, notably the client 304, the server 300 and the NDSMR database 302. In both client 304 and server 300, the basic software is an operating system running on the hardware platform. The platforms and the operating systems of the client and server may differ. Indeed, a key component of the NDSMR system is that through client-server computing a multitude of different types of operating systems may exist within the various medical facility LANs. As long as the client 304 and server 300 share the same communication exchange protocols and support the same applications, the lower-level differences are irrelevant. It is the communications software which enables clients and server to interoperate. Specific to the NDSMR system, the communication exchange protocol adopted will be an open, non-proprietary protocol, for instance the Internet Protocol, a standard exchange protocol in client-server networking, or any other similar progressive communication exchange protocol.

For the purpose of this specification, the term interoperate implies, among other things, the ability of different system users (clients) to share server information and have on-line consultations, in both real and delayed time. Real-time computing is defined as the type of computing in which the correctness of the system depends not only on the logical result of the computation but also on the time at which the results are produced. Real-time tasks therefore attempt to control or react to events that take place in the outside world. As these events occur in "real time", a real-time task must be able to keep up with the events with which it is concerned. On the other hand, delayed-time tasks are not at all concerned with the outside world events, delayed-time system correctness depending solely on the logical result of the computation. The benefits of real-time medical consultations in the case of emergencies are very obvious. Take for example a doctor at Hospital C conferring with a doctor at Hospital D that is remote from Hospital C. Both doctors can share access to an individual's NDSMR, simultaneously studying the record, visible on both of their workstations, and communicating in real-time with each other via some sort of text, voice or video communications link, for instance an Internet messaging window, from their workstations. The equipment necessary to allow for such real-time communication will not be described in detail, as there are a variety of products available on the market that could be used for this task and that are well-known to persons skilled in the art.

The server 300 is responsible for maintaining the NDSMR database, for which purpose a database management system module is required. A variety of different applications that make use of the database may be housed on the client machines. The operative relationship that ties clients, such as client 304, and server 300 together is software that enables a client to make requests to the server 300 for access to the NDSMR database 302. It is important to note that the division of work between a client 304 and server 300 may be allocated in a number of ways. In a preferred embodiment of this invention, the system implements cooperative processing, whereby the application processing is performed in an optimized manner by taking advantage of the strengths of both client and server machines and of the distribution of data. Although such a configuration is quite complex to set up and maintain, in the long run this configuration offers greater user productivity gains and greater network efficiency. Alternatively, the system may be implemented with server-based processing or client-based processing. In server-based processing, the most basic class of client-server configuration, the client is mainly responsible for providing a user-friendly interface, whereas nearly all of the processing is done on the server. In client-server processing, virtually all of the application processing is done at the client, with the exception of certain data validation routines and other database logic functions that are best performed at the server. This latter architecture is perhaps the most common client-server approach in current use. In the interest of clarity, the server-based processing implementation is described in the remainder of this description; however, the NDSMR client-server division of work may be any one of the options described above.

FIG. 7 is a more detailed block diagram of a preferred embodiment of the server 300, which has the responsibility of managing, sorting and searching the NDSMR database 302. Towards this end, the server is provided with a memory 720, high-speed processor/controllers 708, 710 and 712 (assume for this example that there are three), and a high-speed input/output (I/O) architecture. The I/O architecture consists of the interfaces 702, 704 and 706. An internal system bus 711 interconnects these components, enabling data and control signals to be exchanged between them. The server has 6 ports, identified as port A, port B, port C, port D, port E and port F. These ports connect the server to physical links 1, 2 and 3, allowing data to be transported to and from various clients within the network. In the example shown, ports A, B and C are input ports on the physical links 1, 2 and 3, respectively, while ports D, E and F are the output ports on those same physical links. The input ports are designed to receive data from their associated physical links, while the output ports are designed to transmit data over their associated physical links.

The interfaces 702, 704 and 706 interconnect various input and output ports to the physical links 1, 2 and 3, respectively. Their function is to transmit incoming data packets to the internal system bus 711 for transport to the memory 720 where they can be processed by one of the processors. On the output side, the interfaces are designed to accept data packets from the system bus 711 and impress the necessary electrical signals over the respective physical links so that the signal transmission can take effect. It is not deemed necessary to discuss this standard operation of the interfaces 702, 704 and 706 in more detail because it is well known to those skilled in the art and is not critical to the success of the invention.

The memory 720 contains a program element that controls the operation of the server. That program element is comprised of individual instructions that are executed by the controllers, as will be described in detail below. The program element includes several functional blocks that manage several tasks. One of those functional elements is the Database Management System (DBMS) 714 which provides efficient and effective use and maintenance of the NDSMR database 302. The DBMS will not be described in detail because it is well known to those skilled in the technological field to which the present invention belongs.

Besides the program element, the memory also holds the usual routing table that maps the destination addresses of incoming IP data packets (inherent to the IP communications exchange protocol) to the server output ports. It is not deemed necessary to discuss the structure of the routing table here because this component is not critical for the success of the invention and also it would be well known to a person skilled in the technological field to which the present invention belongs. The memory also provides random access storage, capable of holding data elements such as data packets that the processors manipulate during the execution of the program element.

Another component stored in the memory 720 is a validation table, which maps all of the registered user IDs to corresponding passwords. The table is used to validate clients logging on to the server, for security purposes. One of the characteristics of cooperative or client-based processing is that a system feature such as user validation would not necessarily be exclusive to the server, but could also take place, in whole or in part, at the client workstation. This would remove from the server a part or all of the burden of dealing with invalid clients, thus increasing system speed and efficiency. The identification table associates with each user a unique user profile that specifies permissible operations and NDSMR accesses, in order to limit access to data held within the database. Specifically, the table is used to identify between clients with different user privileges, for instance clients with archivist status as opposed to basic user status. Archivist status accords the client with read and write status, including editing and modifying privileges, for updating the NDSMRs. User status limits the client to NDSMR read status only. Finally the memory 720 contains a request queue which is a buffer memory space of the FIFO type, although alternative types of buffer memory space may also be used, that can hold data packets to be sent to one of the controllers for processing. The physical configuration of the buffer does not need to be described in detail because such a component is readily available in the marketplace and the selection of the appropriate buffer mechanism suitable for use in the present invention is well within the reach of a person skilled in the art.

In a most preferred embodiment of this invention, the NDSMR database 302 is part of the memory 720 of the server 300, as shown in FIG. 7. In this embodiment, the NDSMR database 302 is actually on a separate storage medium, such as a non-volatile medium interconnected through a high speed data bus with the memory 720 so the record set from the database 302 can be quickly loaded in the random access memory 720 for processing. Alternatively, the collection of data which makes up the NDSMR database 302 may be stored remotely on one or a set of physical storage device(s), for instance a disk. In such a case, one of the server's device drivers would be responsible for communicating directly with the peripheral device(s) in order to access the database.

FIG. 8 provides a complete flowchart illustrating an example of the operation of the program element stored in the memory **720**, and executed by any one of the processor/controllers, that regulates the operation of the server **300**, specifically its interaction with the clients as well as with the NDSMR database **302**. Although the server program is running at all times, if no clients are logged on to the server then it is in an effective perpetual wait state, shown at step **800**. Once a client attempts to log on, control is passed to the validation functional bloc that is part of the program element in order to ensure that the client is a server registered user at step **804**. Validation consists simply in ensuring that the user's ID is known to the system (exists within the validation table) and that the user knows the correct password associated by the system with that ID (mapped by the validation table). If either the user's ID is not known to the system, or the password given is incorrect, validation will fail and the user refused possibility of logging on to the server. This is a basic validation procedure that is widely used. Evidently, more complex validation methods can be implemented, if the level of security demands it. Next, the server waits for a request from any of the logged on clients at step **806**. When a request does occur, it arrives as a flow of data packets at interface **702**, **704** or **706**, over physical link **1**, **2** or **3**, respectively. At step **810**, the request is stored in the request queue found in memory **720**, to await its turn for processing. The program element next releases a request from the queue (the oldest request) to any non-busy processor. If all of the processors are occupied, the release step is held-up until such a time where any of the three processors is available.

Once a request has been released to a processor, the program element reaches step **814**, whereby the requesting client is identified by the identification logic stored in memory **720**. The identification logic first reads the request data packet header in order to determine the destination address for the response to the request, specifically the address of the requesting client which is read from the source field, and second assigns correct status to the client (user, archivist or other status). This status is determined by the user profile, read from the identification table stored in memory **720**. Step **814** also includes routing logic, whereby the routing table is accessed in the memory **720** in order to determine the correct output port for transmitting a database response to the particular client.

At step **816**, the processor must determine the search parameters specified by the request. These parameters consist in a patient's identifier and/or a list of other qualifiers (for instance a particular treatment, medical condition, age group, sex, etc). Control is passed to the DBMS logic at step **818**, at which point the search is performed on the NDSMR database. The DBMS not only performs the search on all data contained within the NDSMR database, but also controls access to specific records or even portions of records within the database, ensuring that confidential data or specific confidential parts of the data being accessed is masked when returned to the client, based on the user profile determined at step **814**. The data returned by the NDSMR database search is transmitted over the pre-determined output port and to the appropriate client at step **820**.

As indicated above, an aspect of the current invention is the user-friendly interface provided at the client workstation **304**. This interface facilitates the user's attempts at making requests of the server, through easy to follow prompts and an on-line knowledge system to help the user with any questions or problems. The interface allows the user to perform searches or queries on the NDSMR database, using information filters to simplify the extraction of pertinent data from what may be hundreds of thousands of network distributed shared medical records. The interface also allows the user to perform keyword-based Internet-wide searches, transparent to the user. For example, a workstation user could initiate an Internet search for all documents relating to a particular medical condition by simply inputting the name of the medical condition as the keyword, the search results returned to the user being a list of hypertext links to all corresponding Internet documents. Note that different software packages for implementing such an interface feature exist and are currently available in the marketplace. Finally, the interface offers text processing tools, necessary to the editing, publication and merging of all data received from both the Internet and the server **300**. Future variations to the NDSMR system may include a more progressive interface at the client workstation. Specifically, a three-dimensional view of the human body may be available to doctors and consultants logged on to the NDSMR server, used for making requests, medical enquiries and searches.

The Network Distributed Shared Medical Record itself is another element. The NDSMR is an evolving summary medical document for a particular individual, integrated in the form of a network accessible document. By "summary", this implies that the record does not necessarily contain all the information currently found in local network medical archives. Rather it is a compendium of critical medical information pertinent to a particular individual, potentially useful in the medical diagnosis of an individual's state of health and corresponding treatment. The NDSMR is therefore a shared minimal record, offering a common communication interface to medical facilities that may be using incompatible information systems. It has the merit of being able to be consulted easily, at a distance, on an emergency basis, as opposed to the current situation of files archived in a local network but inaccessible to any users in other networks.

In a preferred embodiment of this invention, the NDSMR includes at least one universal or network attributed identifier, distinguishing one record from another, and a dynamically updated list of biological data pertinent to the individual, accessible by pointers referring to the local network where the data is actually being stored. This biological data consists of significant medical documents in an electronic format such as laboratory tests, x-rays, surgical reports, electrographic data, etc. Alternatively, other embodiments of the NDSMR may also include a variety of other medical information pertinent to the individual. FIGS. 6A, 6B and 6C display a possible layout for the NDSMR as a WWW document, presenting several categories of medical information pertinent to an individual, in this example John Doe. The individual's identifier is indicated at the top of the record, as seen in FIG. 6A. FIGS. 6B and 6C display other categories of information, including:

administrative medical data (date of birth, home and work address and phone number, emergency contact, regular physician, etc);

permanent biological data (blood type, genetic markings or deficiencies, tissue antigens, etc);

significant antecedents (family medical history, personal medical history, surgical history, etc);

current medical condition (allergies, medication, etc).

The final category seen in FIG. 6C consists of the dynamically updated links to other biological data. The eight pointers listed refer to other medical documents pertinent to John Doe which are maintained in different local networks, and which can be downloaded from another network site to the client workstation by invoking the downloading operation embedded in the pointer, thus specifying the address of the site (and if necessary of a particular file at that site).

In addition to the set of pointers, the NDSMR could also offer access to complementary external sources of information, transparent to the workstation client. Potential sources could be pharmacy networks, medical libraries or journals, accessible to the doctor or consultant via references within the NDSMR seen on their workstation. Assume a consultant has downloaded John Doe's NDSMR from the server 300, and is verifying the Medication(s) Used reference under the Current Medical Condition category, seen in FIG. 6C. When the consultant invokes the Medication(s) Used reference, for instance by clicking with the computer mouse on the hypertext link, the NDSMR system will automatically generate user authorization in order to access an Internet published Medical Library that may be held on an Internet site containing this information, thus allowing the consultant to look up the specifics concerning John Doe's current medication.

In accordance with this invention, the data structure of the pointer allows the workstation user, such as a doctor or consultant, to determine the general nature of the information to which the pointer is referring. In other words, the doctor can tell by simply looking at the pointer whether it points to a medical document concerning a pulmonary x-ray, an electrocardiogram, allergy tests, etc. In a preferred embodiment of this invention, the pointer representation, as seen on the screen of the client workstation, is as seen in FIG. 6C. The textual representation of the pointer indicates clearly to the user the medical document or information to which the pointer points, whether it be the most recent or a previous electrocardiogram, coronarography, x-ray or brain CT scan. Alternatively, the pointers may be of a graphical representation, small icons used to specify relevant body parts and illustrate medical treatments. The scope of this invention also includes all other variations of a pointer representation implementation which reveals the nature of the information to which it points. Transparent to the user is the actual address, hidden beneath the physical representation, which is the actual device needed for contacting and downloading from various external LANs and other sources, to be discussed in more detail below.

In short, the NDSMR record is a data structure that contains two types of elements, namely a collection of medical data elements about the individual and one or more pointers that allow additional information to be downloaded, this additional information being of a medical nature and complementing the data held in the collection of medical data elements. Specific to this invention, these pointers adopt the URL (Universal Resource Locator) addressing system, allowing to point to a specific file in a directory, where that file and that directory can exist on any machine on the integrated health network and can be served via any of several different methods, specifically the Internet technologies such as ftp, http, gopher, etc. The URL addressing system is well documented and very well known to those skilled in the art, and therefore will not be described in more detail.

Each pointer provides an address which may consist in the entire address information of the file pointed to by the pointer or in a reference to the address information, where the reference may be an index in a table that contains the address information. Associated directly with the pointer is a data field, possibly stored in a mapping table in the memory of the NDSMR server, where this data field contains data indicative of the basic nature of the information held in the file or resource to which the pointer is directed. For the purposes of this specification, the term "associated" implies that the data field is either in a direct one-to-one mapping relationship with the pointer or, alternatively, is integrated with the pointer address to form the actual pointer data structure. In a very specific embodiment, the data field associated with the pointer, indicative of the basic nature of the information pointed to, can contain codes normally used by physicians to categorise treatment events that they have administered to patients. Those codes are normally used for remuneration purposes, however, they can be employed here in a satisfactory manner as indicators of the nature of the medical data. Alternatively, the data field associated with the pointer may also contain the date and time at which the pointer was created (enabling the display of the information at the client workstation to be effected in a chronological order), a textual description of the medical information pointed to, a brief description of the status/results of the medical information pointed to, etc.

To facilitate the reading of the information associated with the pointers, namely the basic nature of the medical data, the display of the pointers may be organized and enhanced to enable the user to easily grasp the meaning of the data without the necessity to refer to lists cross-referencing codes with the basic nature of the medical data. This can be accomplished in several ways. For instance, the pointers related to the same information, for instance containing the address of files that hold electrocardiograms, may be displayed on the client workstation in a separate window and arranged in that window in chronological order. Another possibility is to display besides each pointer an icon or text box with the suitable data. This can be accomplished by providing the clients workstation with a table that maps the code in the pointer identifying the basic nature of the medical data with the type of information to be displayed to the user. When the NDSMR is loaded from the remote server 300, the list of pointers is identified and scanned to extract from them the codes identifying the basic nature of the medical data. The codes are then cross-referenced through the table with the corresponding information to be displayed. The information is then displayed on the screen of the user.

Another aspect of this invention is the update of the NDSMRs, following the creation of new medical data. This task could be effected by a NDSMR administrator, be it a medical archivist, webmaster or some other administrative appointee, also responsible for the maintenance and regular update of a local medical information system. Taking for example the medical archivist, it is known that within all of the healthcare establishments such archivists are currently responsible for ensuring a good upkeep of all local medical files, as well as for producing hospitalization summaries, and therefore are aware of all recent medical acts and treatments performed within their medical facility. An alternative to the use of NDSMR administrators is the implementation of automatic NDSMR updates, a process which would involve the incorporation of some sort of intelligence system into all local medical network information systems.

FIG. 9 illustrates an example of a procedure to be followed by medical facility archivists in order to update the NDSMRs. Assume that the archivist within a particular medical facility receives on a regular basis a list of recent medical acts performed at the facility, as well as supporting documents for these acts. At step 902, the archivist updates the facility's local Intranet medical files and creates updated hospitalization summaries. The archivist's next step is to log on to the NDSMR server, using an archivist assigned password, at step 904. The server and its DBMS will recognize the archivist password and profile and assign privileges accordingly, as described above for steps 804 and

818 of the NDSMR server program element. For each different patient appearing on the archivist's updated list, a request must be made in order to retrieve the appropriate NDSMR. The request is made on the basis of the particular patient's identifier, submitted to the NDSMR server at step **906**. At step **908**, the NDSMR is downloaded to the archivist's workstation, at which point the archivist is capable of modifying and updating certain sections of the data contained in the NDSMR, for instance the Significant Antecedents, Current Medical Condition and Links To Other Biological Data categories as seen in FIG. 6C. At step **910**, the archivist refers to the updated list to update the NDSMR in order to reflect the individual's most recent and pertinent medical information, treatments and corresponding pointers. For example, assume that one of the archivist's list entries is that Mr. John Doe has undergone a new electrocardiogram at Hospital E. The archivist will then change the Most Recent Electrocardiogram reference seen in the Links To Other Biological Data category of Mr. Doe's NDSMR to point to the Hospital E local network, more particularly to the file containing the digitized electrocardiogram.

It is important to note that in order for the NDSMR system to function within an extended network of LANs or local Intranets, all documents referred to by pointers should be archived according to a specific nomenclature and be accessible outside of the LAN. In a most preferred embodiment of this invention, this specific nomenclature consists of that adopted by a state or national medical insurance company, thus ensuring record consistency and successful searches. The pointer addresses, transparent to the user, must also have a specific structure, to be respected by all archivists. In a most preferred embodiment of this invention, the structure of the pointer addresses, all the while respecting the URL addressing system, consists in a combination of a local network and machine address (or domain name), a patient's identifier, and a code taken from a published manual of medical act codes adopted by a state or national medical insurance company. There do exist alternatives to the specific nomenclature and pointer structure used by the NDSMR system, and the scope of this invention includes all other such variations whereby consistency is assured within the system.

Yet another feature of this invention is its use as a search/query engine. Not only can a user perform searches for or queries on NDSMRs within his/her own local Intranet, but also within external sources. NDSMR searches and queries may be performed on two different types of data, and therefore databases: nominative and non-nominative. Non-nominative medical data and databases are accessible to all authorized users, but do not require authorization from the patient whose personal data is being consulted. Nominative medical data and databases require search authorization from both the workstation client, typically a doctor or consultant, and the concerned patient, with the exception of situations where emergency medical care is required. The search requester will be prompted for this authorization through the workstation interface described above, the authorization comprising some form of password, biological signature or smart card. In the case where a search is performed by a user without nominative search authorization, the NDSMR Database Management System (DBMS) will automatically mask any nominative data found in the database response before transmitting it to the client workstation. In summary, the NDSMR system permits the delay-free consultation of pertinent information found within different local files and, for authorized users, offers an integrated research motor which allows for non-nominative research, by object or by concept, on the whole of the accessible databases.

In a specific example, a user of the NDSMR system may perform a search of all of the non-nominative medical data and databases accessible via the server **300** for a particular genetic characteristic. Thus, the search results returned to the user by the NDSMR system in response to this query would comprise all NDSMRs, both local and external to the user's Intranet, containing non-nominative medical data that shares this particular genetic characteristic. As mentioned above, all nominative data within these NDSMRs would be masked by the NDSMR DBMS before transmission of the query response to the client workstation. Advantageously, on a basis of such a query it may be possible to associate one or more health problems experienced by a known population with a particular genetic characteristic shared by the known population, thus furthering medical research.

FIG. **10** displays the query usage allowed by the NDSMR system. From a client workstation, a user may make an initial query of the server **300**. The server's DBMS and database logic allow the NDSMR database **302** to be searched rapidly and efficiently. The database logic is what allows the server to not only retrieve records on behalf of the client but also to perform searches on behalf of the client. We see in FIG. **10** that an initial query returned **300** possible NDSMRs. The system allows the user to send out a second, more narrow query, with a resulting 25 NDSMRs returned. The system is therefore very efficient, especially for massive searches performed across all accessible databases. In a most preferred embodiment of this invention, the query style offered by the workstation interface will be one of relational data searches, such as the style currently offered by the Alta Vista™ web browser. The query style will not be described in detail as it is very well known to a person skilled in the art. Alternatively, many other query styles could be incorporated into the NDSMR search engine, for instance an object-oriented search style.

The structure of the pointers as described above, where both an address part and an associated data part form a pointer, allows the NDSMR system to perform searches on all of the pointers contained within the NDSMR database, representing medical files archived at all of the various local networks connected within the extended health network. As mentioned above, the data structure of the pointers allows the nature of the information to which they point to be determined, either directly from the data structure itself in the case where both the data part and address part of the pointer are integrated to form the data structure of the pointer, or through a one-to-one mapping between the address part of the pointer's data structure and the data part, possibly stored in a mapping table in the memory of the NDSMR server. Consequently, medical searches performed on the NDSMRs will return all database records containing pertinent pointer links. These links will allow the user to research medical data from all over the health network, currently impossible but vital to progressive medical development. Thus a query could be made to extract records based on a key relating to the basic medical information. For example, one could extract the records of all individuals between the age of 25–35 that have undergone a particular therapy. This information is particularly useful in statistical studies.

As mentioned above, the use of a Smart Card as a unique network validated or attributed identifier for the NDSMR system users offers several implementation alternatives to the system. In a specific alternative embodiment of the invention, the Smart Card can be used at the client workstation in order to access the NDSMR database. For example, upon attempting to log onto the NDSMR system, the client, most likely a physician, will be prompted by the NDSMR system server (through the user-friendly interface seen at the workstation) to insert the patient's Smart Card into the workstation's appropriate electronic means. These electronic means read the information contained on the card and can extract the patient's identification. The NDSMR server's program element then passes control to its validation functional block in order to ensure that the patient is a server registered user, as described above. In another example, the NDSMR system server may prompt the client workstation user for two Smart Cards, both the physician's and the patient's, thereby increasing the security of the system.

The Smart Card may provide more than simple user identification. In another alternative embodiment of the invention, a patient's Smart Card contains medical information specific to the patient. In one example, the NDSMR system includes the Smart Card as a storage medium for system user information, with the NDSMR database records consisting strictly in at least one unique identifier and a dynamically updated list of pointers to relevant medical information located at remote locations. In such a system, the patient's Smart Card would contain all other medical information pertinent to the individual, for instance that shown in FIGS. 6A, 6B and 6C (minus the Links To Other Biological Data). Upon logging in to the NDSMR system with a Smart Card (or two), the medical information stored on the patient's Smart Card would appear on the client workstation, along with the list of pointers downloaded from the patient's record in the NDSMR database. In another example, a patient's nominative information could all be stored on the Smart Card, with only the patient's non-nominative information stored in the NDSMR database along with the identifier(s) and the list of pointers. This particular implementation of the system would ensure that no queries/searches performed on the NDSMR database revealed any confidential, nominative patient information.

A patient's Smart Card, or alternatively any other form of portable computer readable storage medium, may also be used to store and maintain all or a portion of the data found in the particular patient's NDSMR, where this data may be nominative, non-nominative, static or dynamic. In such a situation, the NDSMR server offers a continuously available means of update for the Smart Card, the update consisting in reading the latest information from the NDSMR and writing it to the Smart Card via the appropriate electronic means, without changing any of the static or nominative data stored on the card. This implementation would allow a physician, at a hospital external to the NDMSR system's integrated health network, to have access to the individual's pertinent and most recent medical information, the only requirement being that the hospital must have the appropriate electronic means to read the individual's Smart Card. A variety of other NDSMR system implementations also exist, distributing the whole of the patients' medical information between database records and patient Smart Cards or other such portable computer readable storage media, and are included within the scope of this invention.

In yet another example of implementation, a personal communication system (PCS), such as a cellular phone, can be used to access the NDSMR database. Other examples of such a PCS include a web phone, a cellular notepad, an IP television screen or monitor, among others. In this example of implementation, users of the NDSMR system, including patients that are registered with the NDSMR system as well as healthcare professionals, can benefit from convenient, mobile means for accessing and using the NDSMR system.

In this non-limiting example of implementation, the PCS is equipped with the same communication exchange protocol as that in use by the NDSMR server 300, such that a connection may be established between the PCS and the NDSMR server 300. This communication exchange protocol may be the Internet Protocol, or any other similar progressive communication exchange protocol.

As described above, when a client attempts to log into the NDSMR system, the NDSMR server 300 will perform a validation procedure in order to confirm that the client is a registered user of the NDSMR system. In one specific example, this validation procedure consists in the server 300 prompting the user of the PCS for an ID and password that are authenticated by the server 300 on a basis of the validation table. Examples of such an ID include a medical insurance number, a social insurance number, a Smart Card, a network attributed identifier, as well as a digital print of the user or any other type of biologically derived signature.

In another specific example, the PCS provides, or itself acts as, an authentication key to uniquely identify a particular user. In the case of a cellular phone, each cellular phone includes a microchip that may serve as the authentication key. For example, when the cellular phone connects to the NDSMR server 300, the microchip will append to the request for connection a unique signature, recognizable by the server 300 as being associated with a registered user of the NDSMR system. Alternatively, the authentication key may be a unique signature of the microchip validated by a pin number, where the server 300 will prompt the user of the PCS for this pin number, or any other method of singular identification.

In addition to an authentication key, the PCS provides the user with a display over which the user may view medical information and query the NDSMR system. In a specific example, the above-described user-friendly interface is provided by the server 300 to the display of the PCS, where this interface permits the PCS user to make data requests, perform searches or queries on the NDSMR database and perform keyword-based Internet-wide searches, among other options. In the case of a cellular phone, the screen of the cellular phone provides a medium over which a certain amount of information can be displayed. Where a large amount of medical information is to be requested of the NDSMR system by the user, the cellular phone may be linked to a television monitor or to a personal or professional computer workstation, for providing the user with a more appropriate amount of display area.

As in the case of the Smart Card, a PCS of a patient registered with the NDSMR system may include a memory device that contains medical information specific to the patient. In one example, the NDSMR system includes the memory device of the PCS as a storage medium for system user information, with the NDSMR database records consisting strictly in at least one unique identifier and a dynamically updated list of pointers to relevant medical information located at remote locations. In such a system, the patient's PCS would contain, in its memory device, all other medical information pertinent to the individual. When a patient logs in to the NDSMR system via his/her PCS, the medical information stored in the patient's PCS would appear on the PCS display, along with the list of pointers downloaded from the patient's record in the NDSMR database. In another example, a patient's nominative information could all be stored in the memory device of the PCS, with only the patient's non-nominative information stored in the NDSMR database along with the identifier(s) and the list of pointers. This particular implementation of the system would ensure that no queries/searches performed on the NDSMR database revealed any confidential, nominative patient information.

In a specific, non-limiting example, the microchip of a cellular phone belonging to a patient registered with the NDSMR system is used as a storage medium to store and maintain all or a portion of the data found in the particular patient's NDSMR, where this data may be nominative, non-nominative, static or dynamic. The data stored on the microchip may be updated on a request basis where, pursuant to logging in to the NDSMR system, a request is sent from the cellular phone to the NDSMR server for updating of the data being maintained on the microchip of the phone. Alternatively, the data stored on the microchip may be updated automatically whenever new pertinent medical information for the particular patient has been archived on the NDSMR server. Specifically, the NDSMR server **300** is capable to offer a continuously available means of update to all of the cellular phone users having subscribed to such a service either directly, through their medical insurance company or through a medical plan under which they are protected.

Taking the example of a cellular phone user that has subscribed to the service directly, when the server **300** is performing the automatic update it will read the latest medical information from the patient's NDSMR and will transmit this data to the patient's cellular phone. In order to perform the data transmission, the server **300** will first attempt to establish a connection with the patient's cellular phone. Once a connection is established, the server **300** will transfer the pertinent medical information to the microchip of the cellular phone, without changing any of the static or nominative data stored in the microchip.

Note that, in addition to being used as a means for accessing the NDSMR system, a PCS may also be used to access any health Intranet that provides distributed medical information and offers to registered users of the Intranet the possibility of connecting by means of a PCS. Such a health Intranet may include a summary medical record database similar to the NDSMR database, where each summary medical record necessarily includes at least one universal or network attributed identifier, distinguishing one record from another, as well as medical information pertinent to the individual associated with the record. This medical information may be in the form of:

textual data;

textual data and a dynamically updated list of biological data pertinent to the individual, accessible by one or more pointers addressing one or more remote databases where the data is actually being stored;

textual data and multimedia information;

among other possibilities.

As in the case of the NDSMR system, the biological data that is accessible by pointers may consist of significant medical documents in an electronic format, such as laboratory tests, x-rays, surgical reports, electrographic data, etc.

The above detailed description of examples of implementation under the present invention should not be read in a limitative manner as refinements and variations are possible without departing from the spirit of the invention. The scope of the invention is defined in the appended claims and their equivalents.

I claim:

1. A mobile communications system for accessing a network system managing medical information, the network system including a server storing a plurality of summary medical records associated with respective individuals, each summary medical record containing the most recently available medical information for the respective individual, said mobile communications system comprising:

an interface for exchanging data with a user;

a processor;

a memory storing a program element including individual instructions for execution by said processor, said program element being responsive to one or more commands input by the user via said interface to:

a) establish a data communications pathway between said mobile communications system and the server of the network system;

b) generate a request associated with a particular summary medical record stored in the server of the network system;

c) transmit said request to the server over the data communications pathway;

d) receive at least a portion of the medical information contained in the particular summary medical record from the server over the data communications pathway; and

e) transmit said at least a portion of the medical information contained in the particular summary medical record to the user via said interface.

2. The mobile communications system as defined in claim **1**, wherein the network system implements a validation procedure for validating users attempting to access the server, said program element being further operative to execute the validation procedure once said data communications pathway has been established by sending to the server unique identification data associated with said mobile communications system.

3. The mobile communications system as defined in claim **2**, wherein said unique identification data includes an identifier and a password.

4. The mobile communications system as defined in claim **3**, wherein at least one of said identifier and said password is selected from the group consisting of a medical insurance number, a social insurance number, a Smart Card, a network attributed identifier and a digital print of the user.

5. The mobile communications system as defined in claim **3**, wherein said identifier and said password are obtained from the user of said mobile communications system via said interface.

6. The mobile communications system as defined in claim **2**, wherein said unique identification data is an authentication key of said mobile communications system.

7. The mobile communications system as defined in claim **6**, wherein said authentication key is a unique signature of said mobile communications system.

8. The mobile communications system as defined in claim **7**, wherein said unique signature is accompanied by a pin number obtained from the user of said mobile communications system via said interface.

9. The mobile communications system as defined in claim **6**, wherein said authentication key is a unique signature of a microchip in said mobile communications system.

10. The mobile communications system as defined in claim **1**, wherein said memory of said mobile communications system is capable of storing locally medical information specific to a particular individual.

11. The mobile communications system as defined in claim **10**, wherein said medical information stored locally in said memory includes at least a portion of the summary medical record associated with the particular individual in the server of the network system.

12. The mobile communications system as defined in claim 10, wherein said memory stores nominative information specific to the particular individual.

13. The mobile communications system as defined in claim 10, wherein said mobile communications system is operative to access the server of the network system in order to update the medical information stored locally in said memory.

14. The mobile communications system as defined in claim 13, wherein said mobile communications system is operative to transmit a request to the server of the network system to update the medical information stored locally in said memory.

15. The mobile communications system as defined in claim 10, wherein the medical information stored locally in said memory is updated automatically by the network system when new medical information specific to the particular individual is archived on the server of the network system.

16. The mobile communications system as defined in claim 1, wherein said mobile communications system is a personal communications system.

17. The mobile communications system as defined in claim 16, wherein said personal communications system includes a display.

18. The mobile communications system as defined in claim 17, wherein said interface is provided by the server of the network system to the display of said personal communications system.

19. The mobile communications system as defined in claim 18, wherein said interface permits the user to provide a plurality of different commands directly to the server of the network system.

20. The mobile communications system as defined in claim 19, wherein the different commands are selected from the group consisting of data request, search or query on the network system, and keyword-based Internet search.

21. The mobile communications system as defined in claim 22, wherein said display is the screen of the cellular phone.

22. The mobile communications system as defined in claim 17, wherein said personal communications system is a cellular phone.

23. The mobile communications system as defined in claim 16, wherein said personal communications system is selected from the group consisting of a web phone, a cellular notepad, and an Internet Protocol television or monitor.

24. In combination:

a network system including a server storing a plurality of summary medical records associated with respective individuals, each summary medical record containing the most recently available medical information for the respective individual; and

a mobile communications system comprising:

a) an interface for exchanging data with a user,

b) a processor, and

c) a memory storing a program element including individual instructions for execution by said processor, said program element being responsive to one or more commands input by the user via said interface to:

i) establish a data communications pathway between said mobile communications system and said server,

ii) generate a request associated with a particular summary medical record stored in said server,

iii) transmit said request to said server over the data communications pathway,

iv) receive at least a portion of the medical information contained in the particular summary medical record from said server over the data communications pathway, and

v) transmit said at least a portion of the medical information contained in the particular summary medical record to the user via said interface.

25. A method for using a mobile communications system to access a network system managing medical information, the network system including a server storing a plurality of summary medical records associated with respective individuals, each summary medical record containing the most recently available medical information for the respective individual, said method comprising:

establishing a data communications pathway between the mobile communications system and the server of the network system;

generating a request associated with at least one summary medical record stored in the server of the network system;

transmitting said request to the server over the data communications pathway;

receiving at least a portion of the medical information contained in the at least one summary medical record from the server over the data communications pathway; and

transmitting said at least a portion of the medical information contained in the at least one summary medical record received from the server to a user of the mobile communications system.

* * * * *

SKlinger_Job_1_of_1

Printed by HPS Server
for

EAST

Printer: ran_4c70_gbrfptr
Date: 02/07/05
Time: 14:38:32

Document Listing

Document	Selected Pages	Page Range	Copies
US20030131110	12	1 - 12	1
Total (1)	12	-	-

US 20030131110A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0131110 A1**

Chang et al. (43) **Pub. Date: Jul. 10, 2003**

(54) **SYSTEM AND METHOD FOR CONCURRENT SECURITY CONNECTIONS**

(75) Inventors: **David Yu Chang**, Austin, TX (US); **Derek Wan Hok Ho**, Austin, TX (US)

Correspondence Address:
Joseph T. Van Leeuwen
P.O. Box 81641
Austin, TX 78708-1641 (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(21) Appl. No.: **10/042,495**

(22) Filed: **Jan. 9, 2002**

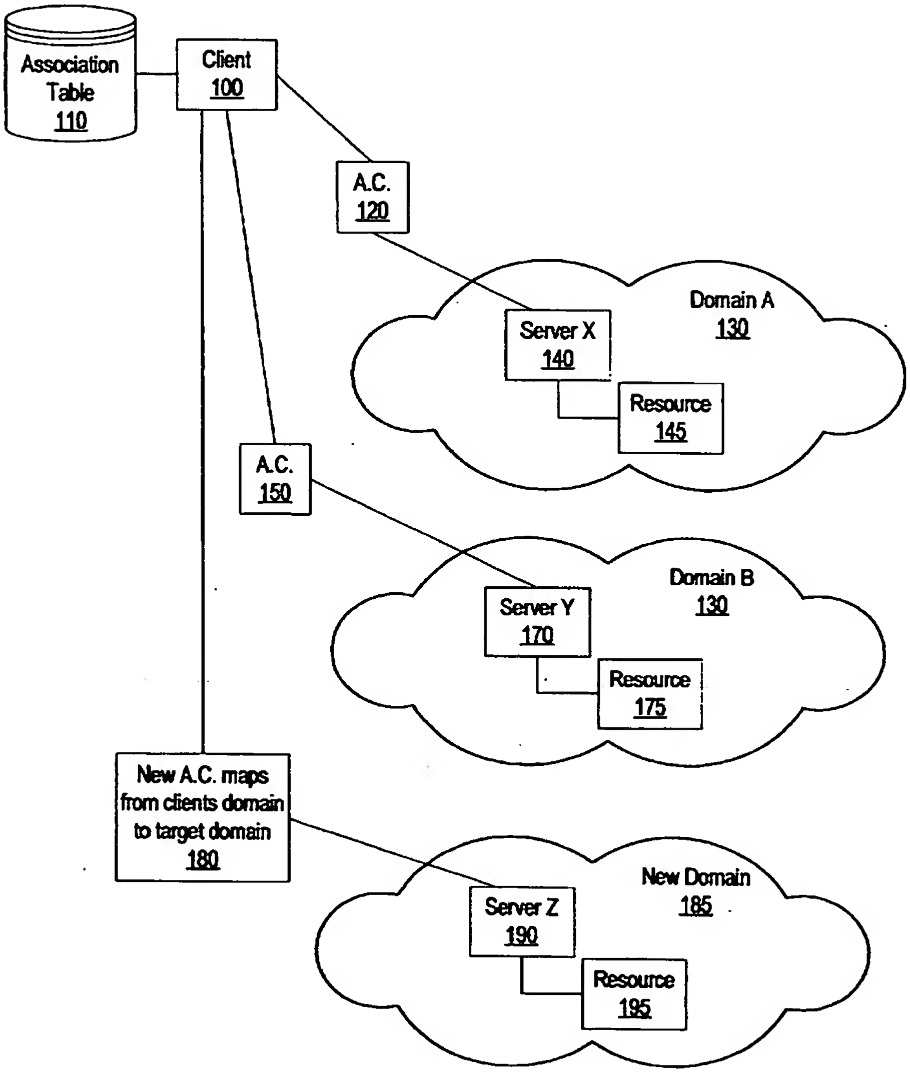
Publication Classification

(51) **Int. Cl.^{7}** **G06F 15/16**

(52) **U.S. Cl.** **709/227**

(57) **ABSTRACT**

A system and method for concurrent security connections is presented. An association table is used that includes a list of active credentials. An active credential includes information such as user id and password information for a given domain. The active credential may also include dynamic data that is retrieved from a user, such as a pseudo-random code or a fingerprint scan. The active credential is sent to a domain, or the managing server of the domain, when domain access is requested. This access request does not involve the user of the client unless dynamic input data is requested.



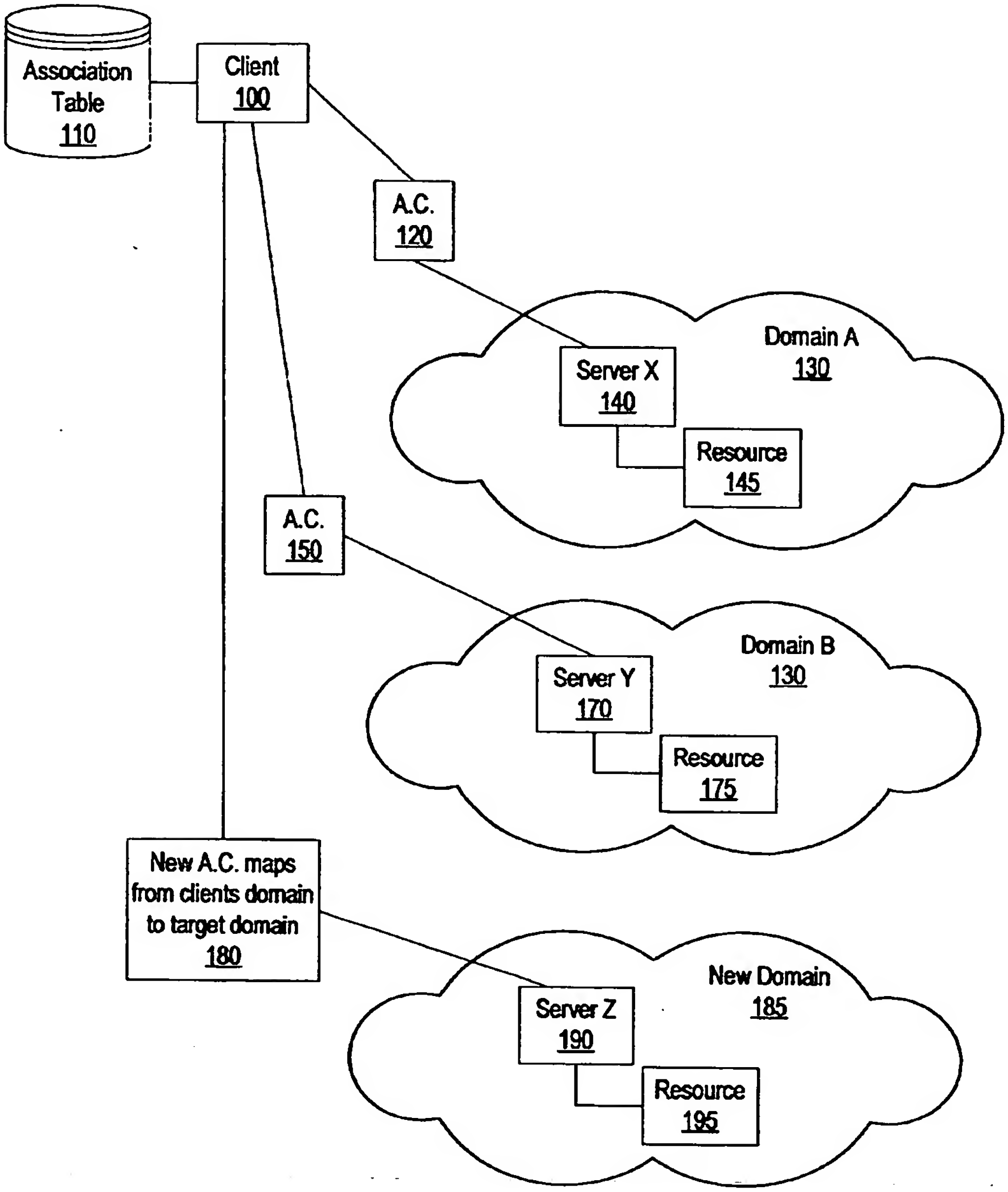

Association Table 110
Client 100
A.C. 120
Domain A 130
Server X 140
Resource 145
A.C. 150
Domain B 130
Server Y 170
Resource 175
New A.C. maps from clients domain to target domain 180
New Domain 185
Server Z 190
Resource 195

Figure 1

DOMAIN 210	SERVER 220	USER ID 230	PASSWORD 240	DYNAMIC DATA 250	TOKEN 280	HOST NAME 290
A	X	JOHND	XYZ12		<Key> 283	<IP Addr.> 293
B	Y	JDOE	1XYZ789		<Data Struct> 286	<Name> 296
C	Z	JOHNDOE	XYZ789	<Data Desc.> 270		

260

Association Table
200

Figure 2

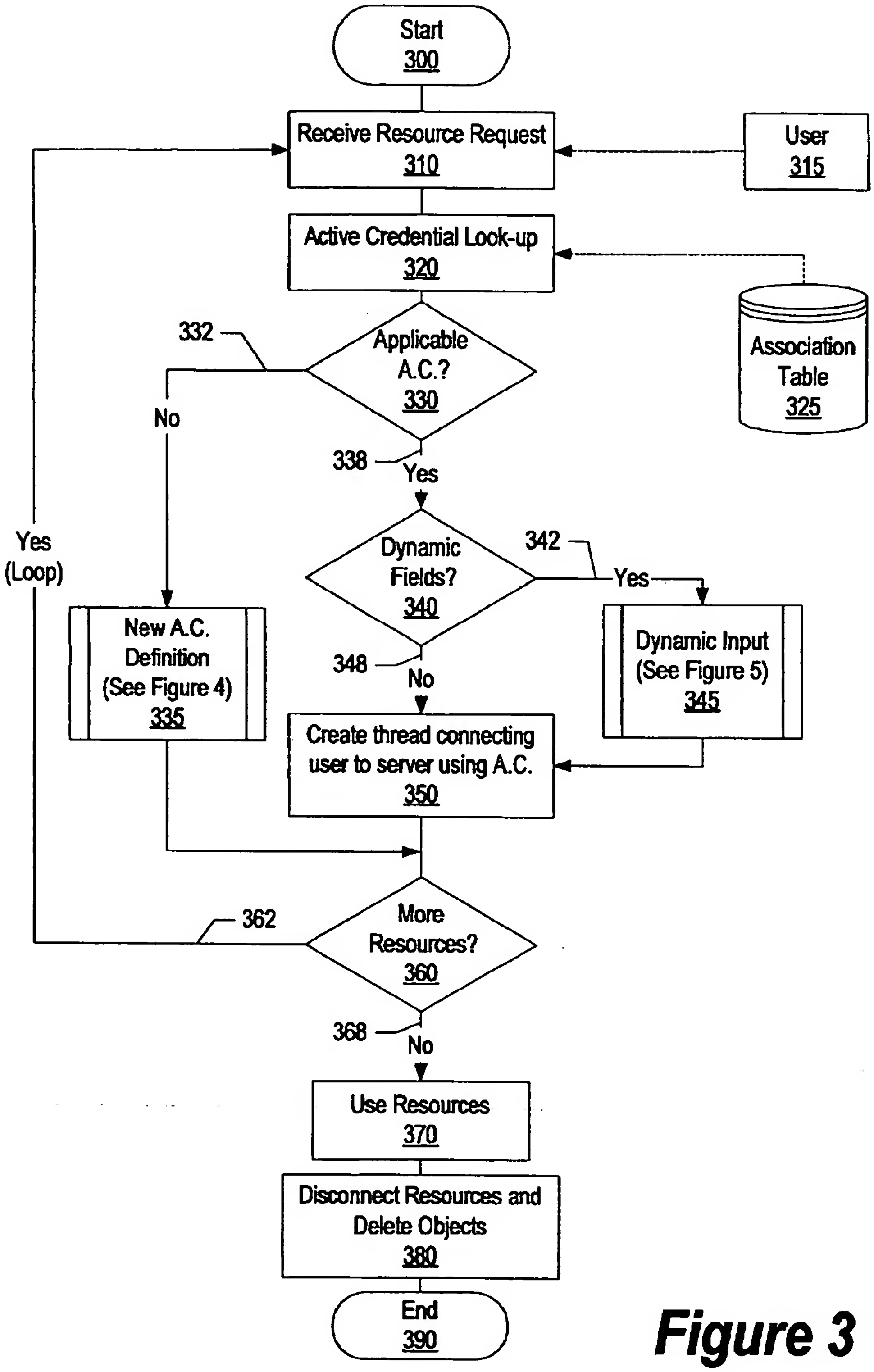

Start
300
Receive Resource Request
310
User
315
Active Credential Look-up
320
Association Table
325
332
Applicable A.C.?
330
No
338
Yes
Yes (Loop)
Dynamic Fields?
340
342
Yes
New A.C. Definition (See Figure 4)
335
348
No
Dynamic Input (See Figure 5)
345
Create thread connecting user to server using A.C.
350
362
More Resources?
360
368
No
Use Resources
370
Disconnect Resources and Delete Objects
380
End
390

Figure 3

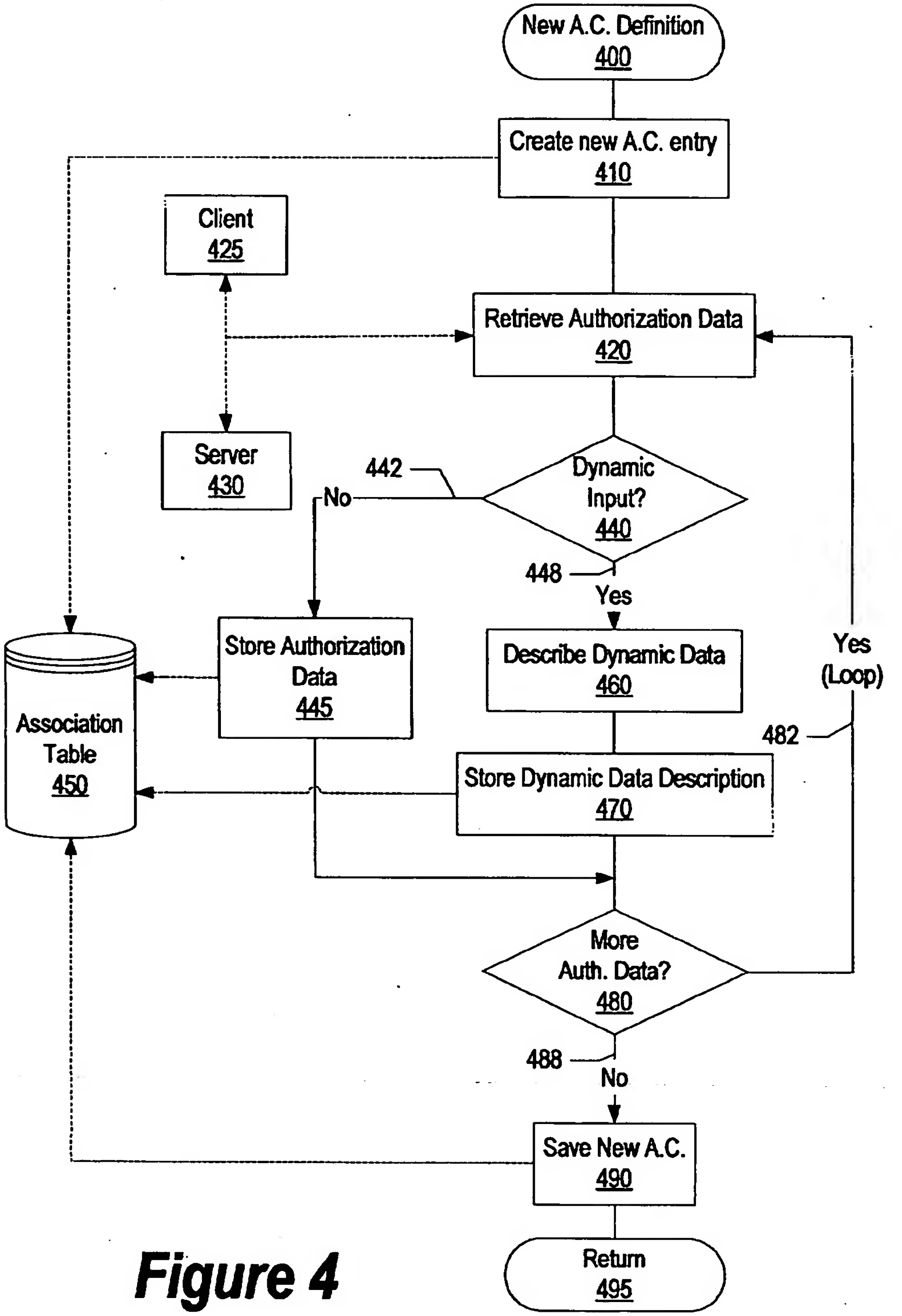

New A.C. Definition
400
Create new A.C. entry
410
Client
425
Retrieve Authorization Data
420
Server
430
442
No
Dynamic
Input?
440
448
Yes
Store Authorization
Data
445
Describe Dynamic Data
460
Yes
(Loop)
Association
Table
450
482
Store Dynamic Data Description
470
More
Auth. Data?
480
488
No
Save New A.C.
490
Return
495

Figure 4

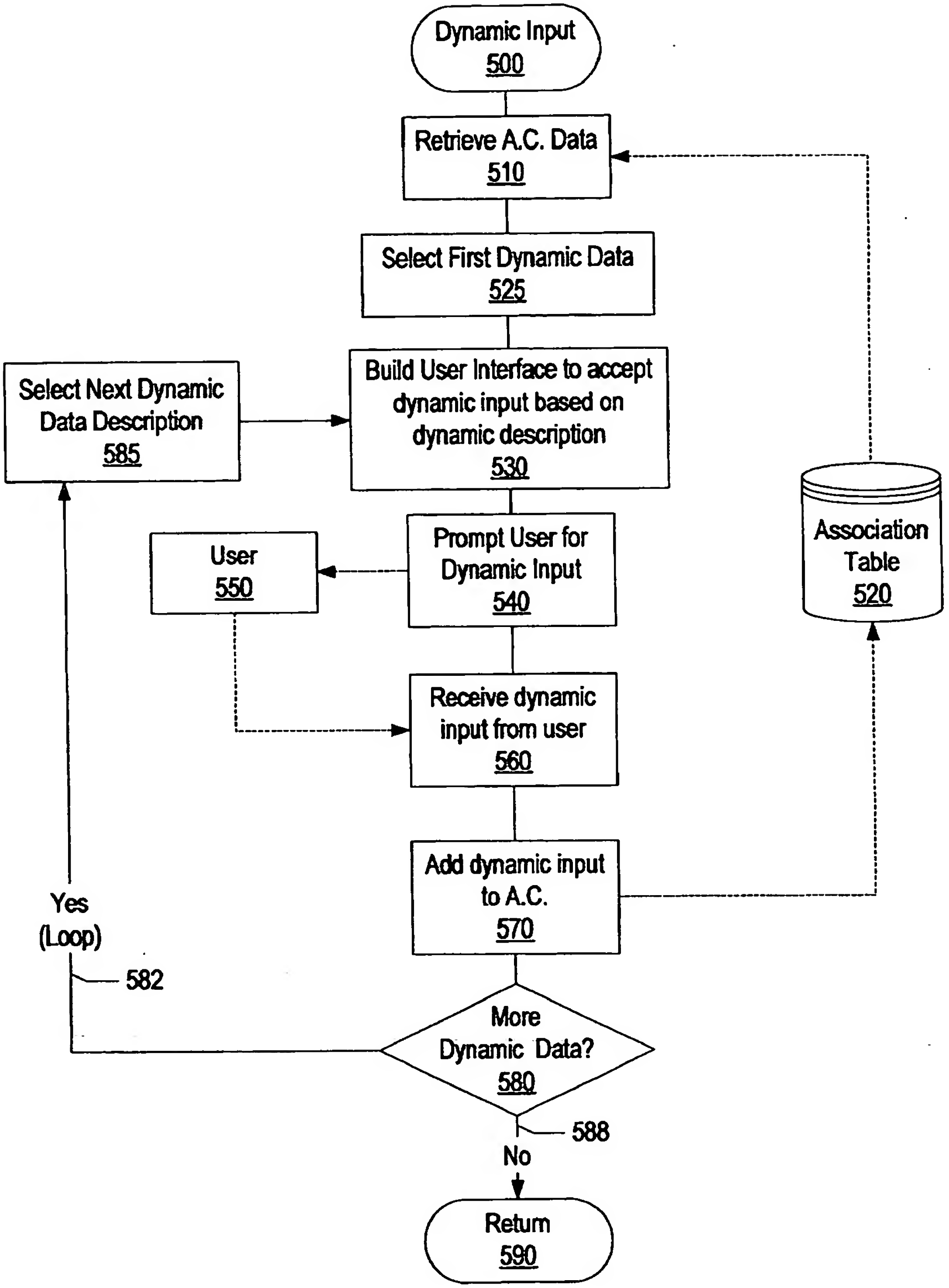

Dynamic Input
500
Retrieve A.C. Data
510
Select First Dynamic Data
525
Build User Interface to accept dynamic input based on dynamic description
530
Select Next Dynamic Data Description
585
Association Table
520
Prompt User for Dynamic Input
540
User
550
Receive dynamic input from user
560
Add dynamic input to A.C.
570
Yes (Loop)
582
More Dynamic Data?
580
588
No
Return
590

Figure 5

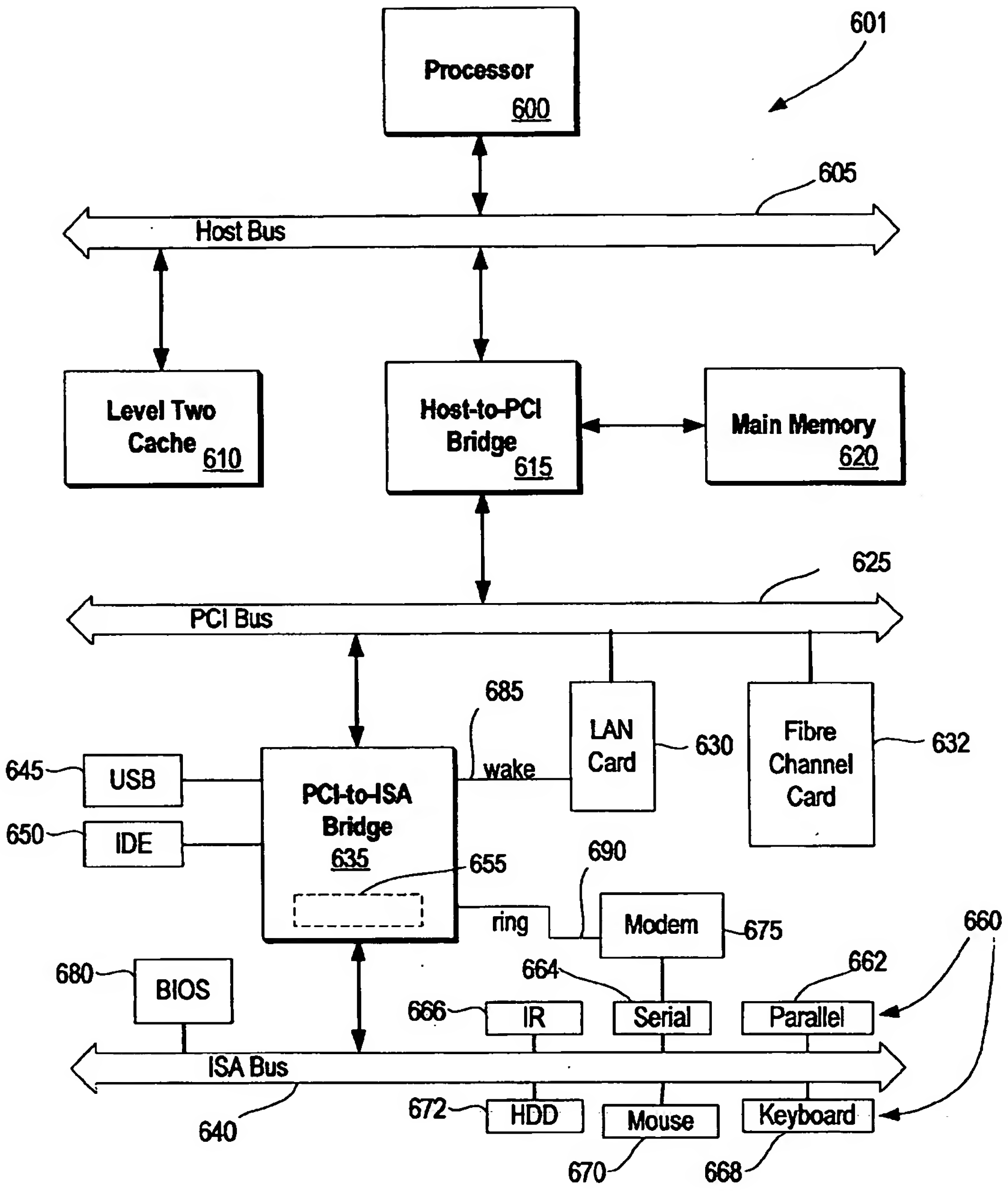

601
Processor
600
605
Host Bus
Level Two Cache
610
Host-to-PCI Bridge
615
Main Memory
620
625
PCI Bus
685
wake
LAN Card
630
Fibre Channel Card
632
645
USB
650
IDE
PCI-to-ISA Bridge
635
655
690
ring
Modem
675
660
680
BIOS
664
662
666
IR
Serial
Parallel
ISA Bus
640
672
HDD
Mouse
Keyboard
670
668

Figure 6

SYSTEM AND METHOD FOR CONCURRENT SECURITY CONNECTIONS

BACKGROUND OF THE INVENTION

[0001] 1. Technical Field

[0002] The present invention relates in general to a method and system for multiple login contexts. More particularly, the present invention relates to a system and method for enabling concurrent security connections in a heterogeneous network.

[0003] 2. Description of the Related Art

[0004] A user may access different networks to retrieve and send information based upon the task at hand. The user may access different networks within his company, especially if the company is large and covers multiple geographic areas. Even though the company may strive to have similar networks throughout the individual business areas, this may be difficult to accomplish in cases where a company purchases another company and attempts to integrate the two networks. The user may also access networks external to his company. For example, an engineer may be designing a system using a vendor's device. The engineer may access proprietary technical notes that are located on the vendor's network through a Virtual Private Network (VPN) or other secure network.

[0005] A network may have varying degrees of logon complexity based on the security needs of the network. For example, a network that includes highly sensitive information may have a very complex login requirement which may include the use of biometric inputs and the use of dynamic encryption cards that synchronize random numbers with login servers at various points in time. A second network in the same company that does not include sensitive information may have a very simple login requirement, such as simply entering a user id and password. Each network may also have specific login security requirements. For example, one network may have a password requirement length of five alpha characters and another network may have a password requirement of eight characters in which two of them are numeric.

[0006] Networks may require a dynamic login method for user's logging in from a remote location in order to have an additional level of security. For example, the network may require that the user enter a number based on a pseudo-random code that changes numbers at specific time intervals, such as with an ACET™ card. The probability that a user encounters a unique logon requirement increases when the user accesses external networks. As mentioned before, some networks may require the contemporaneous entry of biometric information, such as the user's fingerprint or retina scan.

[0007] A challenge found in the current art is securely managing the different user id's and different passwords a user configures to access multiple networks. The user may not want to write down his user id's and passwords for security risk reasons. Logging on to many different networks during the workday is also time consuming and cumbersome. While a user may store login information in a secure place, such as an encrypted file eon the user's computer, the repeated retrieval and maintenance of the information is troublesome.

[0008] However, login security requirements are essential and may not be avoided. Login security requirements protect the network from malicious clients wanting to compromise or disrupt the network. What is needed, therefore, is a way to ensure a level of network security while providing a convenient means for client login in a heterogeneous network.

SUMMARY

[0009] It has been discovered that by using a table of active credentials associated with various domains, clients may concurrently login to different security domains and conveniently maintain multiple associations with multiple servers.

[0010] A client maintains an association table that includes a list of active credentials. An active credential includes information such as user id and password information relating to a given domain. Each active credential corresponds to a domain that the client accesses. When the client requests access to a network resource or a domain, the client's computer system retrieves the corresponding active credential from the association table and sends it to a server that manages the requested domain. The server verifies the login information, and grants access for the requested network resource or a domain to the client.

[0011] A client may request access to a network resource or a domain that does not have an existing active credential stored in the association table. An active credential manager monitors the login exchanges between the client and the server that manages the requested domain. The active credential manager creates a new active credential associated with the requested domain and stores the login exchange information in the new active credential for future access requests.

[0012] Some situations may require the user to enter a dynamic data input for increased security reasons. For example, a user may log in to a domain from a remote location and the user may need to use an ACE™ card that shows a changing pseudo-random code. The active credential associated with this configuration includes a dynamic data description that specifies the user interface requirements in order to obtain the dynamic data during the log on sequence.

[0013] The foregoing is a summary and thus contains, by necessity, simplifications, generalizations, and omissions of detail; consequently, those skilled in the art will appreciate that the summary is illustrative only and is not intended to be in any way limiting. Other aspects, inventive features, and advantages of the present invention, as defined solely by the claims, will become apparent in the non-limiting detailed description set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings. The use of the same reference symbols in different drawings indicates similar or identical items.

[0015] FIG. 1 is a diagram of a client accessing multiple resources;

[0016] FIG. 2 is an association table that includes a plurality of active credentials;

[0017] FIG. 3 is a flowchart showing active credentials enabling resource connections;

[0018] FIG. 4 is a flowchart showing a new active credential being created;

[0019] FIG. 5 is a flowchart showing dynamic input being received and stored corresponding to an active credential; and

[0020] FIG. 6 is a block diagram of an information handling system capable of implementing the present invention.

DETAILED DESCRIPTION

[0021] The following is intended to provide a detailed description of an example of the invention and should not be taken to be limiting of the invention itself. Rather, any number of variations may fall within the scope of the invention which is defined in the claims following the description.

[0022] FIG. 1 is a diagram of a client accessing multiple resources. Client 100 accesses resource 145, resource 175, and resource 195 within domain A 130, domain B 160, and new domain 185, respectively. Client 100 has active credentials corresponding to Domain A 130 and Domain B 160 stored in association table 110. For example, resource 145 may be a printer that client 100 frequently accesses and resource 175 may be a time card system that client 100 accesses weekly. Association table 110 is located in a non-volatile storage area, such as a computer hard drive, accessible by the client.

[0023] Client 100 requests access to resource 145 that is within domain A 130. Client 100 retrieves an applicable active credential from association table 110 that corresponds to domain A 130. Client 100 sends active credential 120 to server X 140 which manages domain A 130. Server X 140 grants access for Domain A to client 100 and client 100 accesses resource 145.

[0024] Server X 140 may allow access of domain A 130 to client 100 for a specific period of time, or may require client 100 to send authorization information each time client 100 access resource 145. For example, resource 145 may be a printer that client 100 accesses many times during a day. Client 100 sends active credential 120 to server X 140 each time client 100 requests to print a document. The user of client 100 may not be bothered with sending authorization information since the authorization information is included in active credential 120.

[0025] Client 100 requests access to resource 175 that is within domain B 130. Client 100 retrieves an applicable active credential from association table 110 that corresponds to domain B 160. Client 100 sends active credential 150 to server Y 170 which manages domain B 160. Server Y 170 grants access for Domain B to client 100 and client 100 accesses resource 175. Server Y 170 may allow access of domain B 160 to client 100 for a specific period of time, or may require client 100 to send authorization information each time client 100 access resource 175. For example, resource 175 may be a timecard system that the user of client 100 accesses once a week to enter the amount of hours the user worked during the week. Client 100 sends active credential 150 to server 170 each time the user of client 100 requests to enter timecard information. The user of client 100 may not be bothered with sending authorization information since the authorization information is included in active credential 150.

[0026] In another embodiment, client 100 may be accessing domain B 160 from a remote location. Domain B may require a higher level of security for remote clients. An ACE™ card may be used that provides a changing pseudorandom code that a user may enter into active credential 150. In addition to the other authorization information sent within active credential 150, server Y 170 verifies that the pseudorandom code matches a pseudo-random code maintained by server Y 170 that corresponds to the client's userid. After authorization is complete, server Y 170 grants access to client 100.

[0027] Client 100 requests access to resource 195. Client 100 access association table 110 and determines that an active credential is not defined that corresponds to new domain 185. For example, domain 185 may be a vendor's domain and resource 195 includes technical notes of a device that the vendor manufactures. Client 100 contacts Server Z 190 which manages new domain 185 and requests access to new domain 185. Client 100 defines new active credential 180 through a login process with Server Z 195 and stores information corresponding to new active credential 180 in association table 110 for future access requests to new domain 185.

[0028] FIG. 2 is an association table that includes a number of active credentials. Association table 200 includes various fields that are used to allow a client access to various resources. Domain field 210 includes information about the domain that corresponds to a given resource. For example, domain field 210 shows domain A, domain B, and domain C are registered in association table 200. Server field 220 includes information about a server that controls the corresponding domain. For example, server X, server Y, and server Z correspond to domain A, domain B, and domain C, respectively.

[0029] User id field 230 includes an applicable user id that allows the client to access the corresponding server. For example, JOHND, JDOE, and JOHNDOE are the user id's that correspond to server X, server Y, and server Z, respectively. Password field 240 includes an applicable password that corresponds to the user id in the same active credential. For example, XYZ12, 1XYZ789, and XYZ789 correspond to user id's JOHND, JDOE, and JOHNDOE, respectively.

[0030] Dynamic data field 250 includes information about dynamic information required for a given active credential. For example, active credential 260 requires users to enter dynamic data information corresponding to dynamic data description 270. Data description 270 may inform the user to enter a pseudo-random code on his ACE™ card in order to access domain C.

[0031] Token field 280 includes additional security information, such as key 283 and security data structure 286. Key 283 may include a shared private key or a public key/private key (i.e., a private key used to authenticate the client with a message deciphered by a server using the client's public key, or a public key corresponding to the server that is used to authenticate the server).

[0032] Host name field **290** can include an address of a host computer system. Examples of host computer system addresses include IP address **293** and string name **296** which each identify a host computer by an address. The host name can be used for delegation whereby a server computer system uses association table **200** in order to act on behalf of a client computer system (i.e., the client computer system delegates the server to perform certain actions that require the server to access one or more computer resources for which client authentication information is required).

[0033] **FIG. 3** is a flowchart showing resources being accessed using active credentials. Processing commences at **300**, whereupon a resource request is received from user **315** (step **310**). Association table **325** is searched to find an active credential that matches the requested resource (step **320**). A determination is made as to whether an active credential is retrieved that is applicable to the requested resource (decision **330**). If the active credential is not applicable, decision **330** branches to "No" branch **332** whereupon a new active credential is defined (pre-defined process block **335**, see **FIG. 4** for further details). On the other hand, if the active credential is applicable, decision **330** branches to "Yes" branch **338** whereupon a determination is made as to whether the active credential has dynamic field requirements (decision **340**).

[0034] If the active credential has dynamic field requirements, decision **340** branches to "Yes" branch **342** whereupon the dynamic field is processed (pre-defined process block **345**, see **FIG. 5** for further details). On the other hand, if the active credential does not have dynamic field requirements, decision **340** branches to "No" branch **348** bypassing the dynamic input processing. After the security information has been gathered, a thread is created using the active credential that connects the user to the requested resource using the retrieved security information (step **350**).

[0035] A determination is made as to whether the user requests more resources (decision **360**). If the user requests more resources, decision **360** branches to "Yes" branch **362** which loops back to receive another resource request. This looping continues until there are no more resource requests, at which point decision **360** branches to "No" branch **368**. The resources are used at step **370**. When the resources are no longer used, the resources are disconnected from the client's computer system at step **380**, and processing ends at step **390**.

[0036] **FIG. 4** is a flowchart showing a new active credential being created. Processing commences at **400**, whereupon a new active credential entry is created in association table **450**. Authorization data is retrieved during an authorization session between client **425** and server **430** (step **420**). Authorization data may include a user id, a password, a server name, etc.

[0037] A determination is made as to whether the retrieved authorization data includes dynamic data. For example, the retrieved authorization data may request that the user enter a pseudo-random code or a biometric signature, such as a finger print scan. If the authorization data does not include dynamic data, decision **440** branches to "No" branch **442** whereupon the retrieved authorization data is stored in the corresponding active credential located within association table **450** (step **445**). On the other hand, if the authorization data is dynamic, decision **440** branches to "Yes" branch **448** whereupon the dynamic data is described (step **460**). For example, the dynamic data description may include the properties for a user interface to prompt the user for dynamic data, such as a pseudo-random code or a finger print scan. The dynamic data description is stored in association table **450** at step **470**.

[0038] A determination is made as to whether there is more authorization data to retrieve (decision **480**). If there is more authorization data, decision **480** branches to "Yes" branch **482** which loops back to retrieve more authorization data. On the other hand, if there is not more authorization data, decision **480** branches to "No" branch **488** whereupon the new active credential is stored in association table **450** (step **490**), and processing returns at **495**.

[0039] **FIG. 5** is a flowchart showing dynamic input being received and stored with an active credential. Dynamic input processing commences at **500**, whereupon the active credential associated with a resource request is retrieved from association table **520** (step **510**). A user interface is constructed corresponding to the type of dynamic input required (step **530**). For example, the user interface may ask the user to enter a pseudo-random code that is shown on his personalized ACE™ card. Biometric technology may also be used whereby the user interface may request the user to place his thumb on a thumb print scanner.

[0040] Processing prompts user **550** for the dynamic input at step **540**. The dynamic input is received from user **550** (step **560**), and is stored in an active credential that is associated with the requested resource (step **570**). Using the example above, the thumbprint scanner digitizes the user's thumbprint and stores the digitized sample in the corresponding active credential.

[0041] A determination is made as to whether there is more dynamic data to corresponding to the active credential (decision **580**). If there is more dynamic data to describe, decision **580** branches to "Yes" branch **582** which loops back to select the next dynamic data description (step **585**). This looping continues until there is no more dynamic data to describe, at which point decision **580** branches to "No" branch **588**. Processing returns at **590**.

[0042] **FIG. 6** illustrates information handling system **601** which is a simplified example of a computer system capable of performing the server and client operations described herein. Computer system **601** includes processor **600** which is coupled to host bus **605**. A level two (L2) cache memory **610** is also coupled to the host bus **605**. Host-to-PCI bridge **615** is coupled to main memory **620**, includes cache memory and main memory control functions, and provides bus control to handle transfers among PCI bus **625**, processor **600**, L2 cache **610**, main memory **620**, and host bus **605**. PCI bus **625** provides an interface for a variety of devices including, for example, LAN card **630**. PCI-to-ISA bridge **635** provides bus control to handle transfers between PCI bus **625** and ISA bus **640**, universal serial bus (USB) functionality **645**, IDE device functionality **650**, power management functionality **655**, and can include other functional elements not shown, such as a real-time clock (RTC), DMA control, interrupt support, and system management bus support. Peripheral devices and input/output (I/O) devices can be attached to various interfaces **660** (e.g., parallel interface **662**, serial interface **664**, infrared (IR) interface **666**, keyboard interface **668**, mouse interface **670**, and fixed disk (HDD) 672) coupled to ISA bus 640. Alternatively, many I/O devices can be accommodated by a super I/O controller (not shown) attached to ISA bus 640.

[0043] BIOS 680 is coupled to ISA bus 640, and incorporates the necessary processor executable code for a variety of low-level system functions and system boot functions. BIOS 680 can be stored in any computer readable medium, including magnetic storage media, optical storage media, flash memory, random access memory, read only memory, and communications media conveying signals encoding the instructions (e.g., signals from a network). In order to attach computer system 601 to another computer system to copy files over a network, LAN card 630 is coupled to PCI bus 625 and to PCI-to-ISA bridge 635. Similarly, to connect computer system 601 to an ISP to connect to the Internet using a telephone line connection, modem 675 is connected to serial port 664 and PCI-to-ISA Bridge 635.

[0044] While the computer system described in FIG. 6 is capable of executing the invention described herein, this computer system is simply one example of a computer system. Those skilled in the art will appreciate that many other computer system designs are capable of performing the invention described herein.

[0045] One of the preferred implementations of the invention is an application, namely, a set of instructions (program code) in a code module which may, for example, be resident in the random access memory of the computer. Until required by the computer, the set of instructions may be stored in another computer memory, for example, on a hard disk drive, or in removable storage such as an optical disk (for eventual use in a CD ROM) or floppy disk (for eventual use in a floppy disk drive), or downloaded via the Internet or other computer network. Thus, the present invention may be implemented as a computer program product for use in a computer. In addition, although the various methods described are conveniently implemented in a general purpose computer selectively activated or reconfigured by software, one of ordinary skill in the art would also recognize that such methods may be carried out in hardware, in firmware, or in more specialized apparatus constructed to perform the required method steps.

[0046] While particular embodiments of the present invention have been shown and described, it will be obvious to those skilled in the art that, based upon the teachings herein, changes and modifications may be made without departing from this invention and its broader aspects and, therefore, the appended claims are to encompass within their scope all such changes and modifications as are within the true spirit and scope of this invention. Furthermore, it is to be understood that the invention is solely defined by the appended claims. It will be understood by those with skill in the art that if a specific number of an introduced claim element is intended, such intent will be explicitly recited in the claim, and in the absence of such recitation no such limitation is present. For a non-limiting example, as an aid to understanding, the following appended claims contain usage of the introductory phrases "at least one" and "one or more" to introduce claim elements. However, the use of such phrases should not be construed to imply that the introduction of a claim element by the indefinite articles "a" or "an" limits any particular claim containing such introduced claim element to inventions containing only one such element, even when the same claim includes the introductory phrases "one or more" or "at least one" and indefinite articles such as "a" or "an"; the same holds true for the use in the claims of definite articles.

What is claimed is:

1. A method of establishing concurrent network connections, said method comprising:

receiving a resource request;

identifying an active credential from a plurality of stored active credentials;

retrieving the active credential in response to the identifying; and

accessing the requested resource using the retrieved active credential.

2. The method as described in claim 1 further comprising:

defining a new active credential in response to not identifying the active credential.

3. The method as described in claim 1 wherein the active credential includes a dynamic data field.

4. The method as described in claim 3 further comprising:

accepting authorization data corresponding to a network connection;

determining whether the authorization data includes dynamic data; and

storing a dynamic data description based on the determination.

5. The method as described in claim 4 further comprising:

prompting a user for dynamic input based on the dynamic data description;

storing the dynamic input in the dynamic data field within the active credential;

sending the active credential to a computer network corresponding to a login session; and

accessing the computer network.

6. The method as described in claim 1 wherein the stored active credential includes one or more definition fields.

7. The method as described in claim 6 wherein the definition fields are selected from the group consisting of a domain name, a server name, a user id, and a password.

8. An information handling system comprising:

one or more processors;

a memory accessible by the processors;

one or more nonvolatile storage devices accessible by the processors;

a concurrent network connection tool to execute network connections, the concurrent network connection tool including:

means for receiving a resource request;

means for identifying an active credential from a plurality of stored active credentials;

means for retrieving the active credential in response to the identifying; and

means for accessing the requested resource using the retrieved active credential.

9. The information handling system as described in claim 8 further comprising:

means for defining a new active credential in response to not identifying the active credential.

10. The information handling system as described in claim 8 wherein the active credential includes a dynamic data field.

11. The information handling system as described in claim 10 further comprising:

means for accepting authorization data corresponding to a network connection;

means for determining whether the authorization data includes dynamic data; and

means for storing a dynamic data description based on the determination.

12. The information handling system as described in claim 11 further comprising:

means for prompting a user for dynamic input based on the dynamic data description;

means for storing the dynamic input in the dynamic data field corresponding to the active credential;

means for sending the active credential to a computer network corresponding to a login session; and

means for accessing the computer network.

13. The information handling system as described in claim 8 wherein the stored active credential includes one or more definition fields and wherein the definition fields are selected from the group consisting of a domain name, a server name, a user id, and a password.

14. A computer program product stored in a computer operable media for executing concurrent network connections, said computer program product comprising:

means for receiving a resource request;

means for identifying an active credential from a plurality of stored active credentials;

means for retrieving the active credential in response to the identifying; and

means for accessing the requested resource using the retrieved active credential.

15. The computer program product as described in claim 14 further comprising:

means for defining a new active credential in response to not identifying the active credential.

16. The computer program product as described in claim 14 wherein the active credential includes a dynamic data field.

17. The computer program product as described in claim 16 further comprising:

means for accepting authorization data corresponding to a network connection;

means for determining whether the authorization data includes dynamic data; and

means for storing a dynamic data description based on the determination.

18. The computer program product as described in claim 17 further comprising:

means for prompting a user for dynamic input based on the dynamic data description;

means for storing the dynamic input in the dynamic data field corresponding to the active credential;

means for sending the active credential to a computer network corresponding to a login session; and

means for accessing the computer network.

19. The computer program product as described in claim 14 wherein the stored active credential includes one or more definition fields.

20. The computer program product as described in claim 19 wherein the definition fields are selected from the group consisting of a domain name, a server name, a user id, and a password.

* * * * *